

Safeguarding DIA

Interview with
Timothy C. McNeil
Chief, Counterintelligence
and Security Office

- Work Group Breaks Deconfliction Mold
- The Best of the Best Practice for the Worst
- KISS My PowerPoint — Keep It Simple
- EUCOM JAC Enlisted Leader Meets WWII Counterpart





LTG Ronald L. Burgess Jr.
 Director, DIA

Letitia "Tish" Long
 Deputy Director, DIA

Donald L. Black
 Chief, Public Affairs

Jane A. McGehee
 Chief, Internal Communications

Dana M. Black
 Managing Editor

Margan C. Kerwin
 Lorette A. Murray
 Jennifer M. Redding
 Editorial Staff

Brian D. Nickey
 Design/Layout

Graphic Design and Publishing Services
 Branch
 Printing and Posting

DIA's Communiqué is an authorized agency information publication, published for employees of DIA and members of the defense intelligence community. Contents of the Communiqué are not necessarily the official views of, or endorsed by, the U.S. government or the Department of Defense. Articles are edited for style, content and length. Correspondence should be addressed to: DIA Communiqué, Public Affairs Office, Bldg 6000, Washington, DC 20340-5100. Telephone: 703-695-0071 (DSN: 225-0071). The DIA Public Affairs Office welcomes your comments, which may be e-mailed to our Internet address at DIA-PAO@dia.mil or to our JWICS e-mail address at diem200-DIA@dodis.ic.gov.



www.dia.mil

Article Submission Deadlines

Jan./Feb. 2010 issue — Dec. 2, 2009

March/April 2010 issue — Jan. 27, 2010

november/december 2009

HEADLINES

Work Group Breaks Deconfliction Mold <i>By Harry L. Rogers, DX</i>	2
BRAC Lateral Reassignment Program Retains Employees <i>By Amy Lozinak Buckley and Donna K. Zibreg, HC</i>	3
Make 'Time' for Online Safety <i>By John T. O'Connor, KL</i>	4
Is the Latest Best Practice Really the Best? <i>By David E. Frick, AE</i>	4
Family Support Program Lends a Hand <i>By Amy Lozinak Buckley, HC</i>	5
DIA Reserve Support to JFCOM Joint Training <i>By William D. McConnell, DJ</i>	6
What Sparks Your Compassion? <i>By Malinda D. Worley, DA</i>	7
Who Said Introverted Was a Bad Thing? <i>By Lynn "Ann" Griffith, CS</i>	8
No FEAR: Preserving Model Federal Agency Standards <i>By Mika J. Cross, EO</i>	10
Post of the Month: U.S. Defense Attaché Office Tbilisi <i>By the Directorate for Human Intelligence, DH</i>	11
Language Technology at Your Fingertips <i>By Nicholas A. Bemish and Dr. Jennifer A. DeCamp, HC</i>	13
The Art of Foreign Disclosure <i>By Charles L. Shoemaker, IE</i>	14
FE's Internal Controls Branch Helps to Safeguard DIA <i>By the Internal Controls Branch, FE</i>	15
Protecting DOD's Critical Infrastructure <i>By Jonathan Bonniwell, CE</i>	16



"As an analyst, I've worked closely with the Counterintelligence and Security Office throughout my career. You can read about my experiences on page 22."

EXECUTIVE VISION

Interview with Timothy C. McNeil, Chief of the Counterintelligence and Security Office

By the Communique Staff, CP

18

SAFEGUARDING DIA

Safeguarding DIA: Twenty Years and Counting

By the Counterintelligence and Security Office, DA

22

The Best of the Best Practice for the Worst

By Alexander F. Wojcicki, DA

30

LEADING EDGE

KISS My PowerPoint — Keep It Simple

By Brian D. Nickey, CP

33

COMMUNITY OUTREACH

EUCOM JAC Enlisted Leader Meets WWII Counterpart

By Peter G. Park, EUCOM

34

PROFILES

Professional Profile: Sandra Gemmell

36

PEOPLE ON THE MOVE

Civilian and Military Personnel Update Retirements, Anniversaries and Promotions in June, July and August 2009

By the Office of Human Resources, HC

37



Work Group BREAKS DECONFLICTION Mold

By Harry L. Rogers, DX

The Defense Counterintelligence and Human Intelligence Center brought together service, command and coalition partners to develop an improved process for joint human intelligence reporting and deconfliction.

The Defense Counterintelligence and Human Intelligence Center's (DCHC's) Technology Division (DEO-3) hosted the Afghanistan Source Deconfliction Work Group for a three-day problem-solving "laboratory" at the DIAC in September.

Source deconfliction significantly reduces circular reporting by ensuring a person providing information is not giving the same information to more than one intelligence officer. During the meetings, BG Robert Carr, director of DCHC, highlighted the importance of leveraging technologies to further support joint human intelligence (HUMINT) reporting and deconfliction.

The working group reviewed current source management and deconfliction capabilities and

proposed a technical solution to automate the deconfliction process used in theater. This solution is applicable not only between Four Eyes group partners and NATO team members, but also across wide coalitions such as those present in Afghanistan. The "leap-ahead solution" decided upon in the working group sessions breaks existing doctrine, leads technology and, most importantly, solves the problem.

The problem-solving session was organized at the request of MG Michael Flynn, director of intelligence for the International Security Assistance Force (ISAF) and U.S. Forces Afghanistan (USFOR-A). The group's work resulted in the development of a concept of operations using the HUMINT Management and

Reporting Tool (HMART) and integrated system capabilities for U.S. and coalition forces. Implementation of the solution began in October, with new capabilities to be incrementally added throughout the 2010 fiscal year.

Representatives from USFOR-A and ISAF provided the work group with a thorough understanding of the ISAF force structure in Afghanistan, their existing network connectivity and the specific employment assignments of ISAF HUMINT reporting elements. They also highlighted the extent of manual processes still involved in the deconfliction process, which was the driving force behind the work group.

DCHC subject matter experts led the labs, and relied upon participation from other members of DCHC; ISAF-J2X; USFOR-A J2X, U.S. Central Command J2X, Army G2X; the Office of the Undersecretary of Defense for Intelligence; the Afghanistan-Pakistan Task Force (APTF); Marine Corps Intelligence Systems Development Office; DIA's Canadian and British liaison officers; and the NATO HMART program manager.

DCHC's Technology Division continues to centrally manage the information technology needs and system architecture of the counterintelligence and HUMINT enterprise in close cooperation with each of the services, combatant commands and coalition partners.



Photo by Margan C. Kerwin, CP

The Afghanistan Source Deconfliction Work Group gathered for three days to discuss current source management and deconfliction capabilities in theater.

BRAC Lateral REASSIGNMENT PROGRAM Retains Employees

By Amy Lozinak Buckley and Donna K. Zibreg, HC

The Base Realignment and Closure Lateral Reassignment Program helps DIA employees find the right job at the right location.

Implementation of the 2005 Base Realignment and Closure (BRAC) decisions is moving full-steam ahead, and the Directorate for Human Capital (HC) is onboard to help employees through its BRAC lateral reassignment process.

Through a series of town hall briefings and other venues, it became clear that there were employees who couldn't relocate with their positions. At the same time, many others wanted to move to one of our new BRAC locations: Charlottesville and Quantico, Va., and Fort Meade, Md. In response, the Office of Human Resources (HCH) created a lateral reassignment process to help employees on both sides of the relocation issue.

To request a BRAC lateral reassignment, employees fill out a simple online form and attach their résumé. Panels are scheduled and conducted by directorates with assistance from their servicing Human Capital Support Branch and the Panel Support Team. Panel members review reassignment requests into and out of BRAC positions against position descriptions submitted by managers and make reassignment recommendations to the directorates. Using panel recommendations and feedback from managers who interview employees recommended for reassignment into their offices, directorate deputy directors make final reassignment decisions.

Employees have responded to the opportunity to submit reassignment requests in unexpected numbers. The BRAC lateral reassignment Web site was activated May 4, and by the time the first panel met approximately four weeks later, there were close to 100 employees requesting reassignments. As of early September, there were 165 active requests for reassignment into BRAC positions and 85 requests for reassignment out of these positions, and the numbers continue to grow.

The directorates for Analysis (DI) and MASINT and Technical Collection (DT) have been holding panels since early June with good results. So far, 100 reassignments have been recommended. But DI and DT aren't the only directorates holding panels. HC held a panel in August to review employee requests for reassignment into the Charlottesville Human Capital Support Branch. Other directorates and special offices are also expected to hold BRAC lateral reassignment panels for positions in Charlottesville, Quantico and Fort Meade. Because BRAC guidance requires the transition to be completed with minimal mission impact, employee retention is a primary concern of senior DIA leadership.

"Each successful reassignment represents a valued employee who will remain with the agency and contribute to our mission," said Donna Zibreg, HC BRAC project manager.

Initial feedback has been positive. Greg Novak, from the Joint Intelligence Task Force — Combating Terrorism (JITF-CT), wanted to move to one of the new



positions in Charlottesville and filled out the forms for the lateral reassignment. Soon after, he was notified that he had been selected for a position.

"I can't believe how easy the process really was," said Novak.

Another government agency affected by BRAC even asked for a copy of the DIA lateral reassignment process for its own implementation.

Because of the BRAC lateral reassignment panels, the future looks bright for employees who want to stay in the Washington, D.C., area as well as those who want to relocate to one of our new duty stations. HCH plans to run lateral reassignment panels as long as necessary to ensure that the 2005 BRAC decisions affecting DIA are implemented.

For more information, visit <http://hc.dia.ic.gov/civilian/brac/> or contact Zibreg at (202) 231-4850.

To submit a reassignment request, visit the BRAC Lateral Reassignment site on JWICS at <http://diateams.ne.dodiis.ic.gov/sites/HC/HCHQ3/default.aspx>. Employees without JWICS access may contact Zibreg to submit requests. ☛

Make 'TIME' for Online Safety

By John T. O'Connor, KL

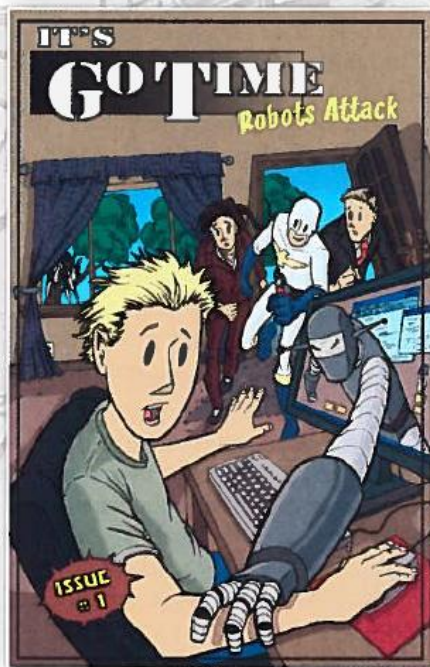
DIA's Knowledge Lab is employing a new way to disseminate critical safety information in a digital age: riveting illustrations, gripping dialogue ... and robots.

A robot reaches its hand out of a computer screen to snare a young boy. In the background, a masked superhero comes to the rescue, along with the boy's parents. On the window sill, a cat is freaking out.

This is the cover of Issue #1 of "It's Go Time: Robots Attack." You may have seen it online or in a distribution stand at the DIAC recently. You might be wondering why DIA has gone into the comics business.

There are two reasons. First, the reality is that DIA is in the counterintelligence and force protection business. The comic book provides information to educate families about the steps they can take to reduce their online vulnerability. The idea is that if our families protect themselves more effectively, that helps to protect the work force and our mission, too. The use of the comic book format also is an experiment to see if we can provide some fun in creating effective learning and knowledge retention.

In recent years the graphic narrative — or comic book — has



grown significantly as a tool for corporate and other communications. Companies such as Google and the National Kidney Foundation have used comics as part of their own business operations. Respected journals like the Harvard Business Review have used them as well. Academic researchers have identified the

comic as an especially effective tool for communicating because, among other qualities, it:

- Translates well to multiple media (print, online, etc.);
- Appeals to a range of audiences (all ages);
- Works in any context (home, office, etc.);
- Can convey depth and complexity;
- Uses simplicity to lead to an emotional impact;
- Leaves audiences wanting more; and
- Creates a brand or enhances branding.

Don't be fooled by the appearance. The content in "It's Go Time" is designed to help make you and your family a harder target for adversaries of all kinds, even evil robots. You can find it online at www.intelink.ic.gov/wiki/Social_Media_Working_Group under "Security Tips for Social Media and Cyberspace," or contact the DIA Knowledge Lab for hard copies at (202) 231-3066. ☛

Is the Latest Best Practice Really the BEST?

By David E. Frick, AE

Could searching for a best practice actually have a negative impact on an organization rather than a positive one?

A best practice is a technique, method, process, activity, incentive or reward that is generally believed to be more

effective at delivering a particular outcome than any other. A best practice may also be couched in terms of efficiency, as opposed

to effectiveness — for example, repeatable processes that have been adopted by a wide range of practitioners over time.

Through the relative ubiquity of the term in business, the phrase has lost some of its edge and has become more popularly used to reflect the generally accepted rules



that business adopts to remain, hopefully, competitive.

I resist the term best practices. Best implies universality, obedience, authority and finality. The debate is over — the matter is closed. In many situations, however, what is best for one organization is impractical for another. Furthermore, if you believe a practice is best, you stop looking for better. Chasing the wrong best practice can have a negative impact. The context of any best practice must be fully understood before it is adopted.

Some consulting firms specialize in propagating best practices. These firms offer premade templates to standardize business process documentation.

Sometimes, simply documenting an organization's process is an improvement, but beware that blindly adopting best practices suggested by the consultant is an abdication of leadership. Once a specific process is anointed as best, poor leaders and managers will tend to change the environment to adapt to the template, instead of changing the template to adapt to the environment. In many cases, the costs of making modifications to the process to fit the standard template exceed the savings realized in adopting the practice. Sometimes a best practice can hurt an organization.

So if the term best practice is not ideal, what is better? The terms good operating practice, better practices or current thinking are coming into vogue. I prefer effective practices or better yet, promising practices. If a practice is promising, you are not disappointed if it fails, and more importantly, you will keep alive the search for a better practice. Words have meaning. Use your words wisely to encourage a culture of continuous process improvement. ☛

Editor's note: Have an opinion you'd like to share? E-mail your articles or letters to the editor to DIA Communication or contact (703) 697-8781.

Family Support Program LENDS A HAND

By Amy Lozinak Buckley, HC

The Office of Human Resource's new program supports employees and their families through difficult times.

"**E**xcellence in defense of the nation" often requires DIA civilian and military employees to be prepared to respond to national security threats anywhere in the world at anytime. To do so, employees must maintain a high degree of readiness and be prepared to deploy at a moment's notice.

In response to DIA's growing need to support its employees and their families during deployments and at home, the Directorate for Human Capital's Office of Human Resources (HC/HCH) has developed a Family Support Program (FSP) that provides services such as family advocacy, crisis response, victim services, work-life balance, deployment support and permanent change of station assistance. DIA's FSP staff is also collaborating with counterparts in the intelligence community and Department of Defense to further develop and implement programs that will enhance the quality of life for agency personnel and their families.

DIA's FSP serves as the coordination point for casualty assistance, as well as coordinating counseling and other services to employee family members. This



Photo by Amy Lozinak Buckley, HC

Work-Life Services' Colleen Betker, left, discusses available DIA programs with a deploying employee and his spouse at a Family Support Night.

daunting task not only includes being on call 24/7, but also requires the FSP to coordinate with DIA's Situation Center to ensure that proper notifications are given to managers in case of personnel injury or death.

In addition to serving as the point of contact for casualty assistance at DIA, the FSP is working to establish a DIA Family Readiness Group (FRG), similar

to the Army's FRG program, to address family and employee concerns relating to deployment separation. DIA's FSP also works closely with the Employee Assistance Program (EAP) to ensure that employees and family members have access to other free counseling services and support programs while separated by a deployment.

Another part of supporting DIA employees and their families is managing the quarterly Family

Support Night at which representatives from EAP, Work-Life Services, and Civilian and Military Pay and Benefits, among other offices, provide information to both the deploying employee and their family staying behind. The goal is to make deployments less stressful for families and employees by providing coping strategies for dealing with issues and concerns before they affect DIA's mission and employee readiness.

Employees are committed to the

agency's mission, and DIA is showing a commitment to its staff by implementing the FSP. By providing employees and their families the tools needed to deal with deployment and related issues, the agency strives to enable employees to focus on the mission at hand.

For more FSP information, contact Kirsten Spevak, family support specialist, at (202) 231-8028 (DSN 428), via JWICS e-mail at kirsten.spevak@dodis.ic.gov, or SIPRNet at kirsten.spevak@dia.smil.mil.

DIA Reserve SUPPORT to JFCOM Joint Training

By William D. McConnell, DJ

Joint Reserve Intelligence Centers offer an affordable solution for supporting the needs of the commands.

In 2008 U.S. Joint Forces Command (JFCOM) identified a need for additional intelligence support from DIA to better support the operational objectives of joint force mission rehearsals. DIA recognized the request, and JFCOM's DIA Forward Element (DFE) began developing alternative solutions to meet their needs. The DFE developed an approach that will simultaneously train reservists, support JFCOM and potentially save the government tens of thousands of dollars.

Joint Force Trainer

JFCOM conducts multiple joint task force (JTF) mission rehearsal events each year in support of the Iraq, Afghanistan and Africa theaters of operation. During these events, hundreds of joint intelligence personnel come together to create a realistic operational environment where the JTF can train.

It is within this construct at JFCOM that DIA personnel get involved. Employees from the directorates for Analysis (DI), Mission Services (DA), and MASINT and Technical Collection (DT), the Defense Intelligence Operations Coordination Center, Defense Counterintelligence and HUMINT Center, Regional Support Centers and the DFEs all participate. DIA provides strategic intelligence to the events, and role-plays several theater and national capabilities to ensure the JTF understands how to leverage our capabilities. The JFCOM DFE began looking for better ways to support the emerging JFCOM requirements and to reduce the costs to DIA.



Author William McConnell stands outside the JFCOM J7 training facility.

Bridging Two Worlds for One Mission

In early 2008 the executive officer of my Navy Reserve unit and I were discussing training and

readiness of deploying units. I explained to him that as a joint trainer I am always looking for better ways to do business, and he asked if I had ever thought of Joint Reserve Intelligence Centers (JRICs).

I learned that a JRIC is a Department of Defense (DOD) SCIF enhanced by the Joint Reserve Intelligence Connectivity Program (JRICP), where reservists and contractors from one or more services fulfill intelligence requirements for national, joint or service customers who are geographically distant. The JRIC sites can also support any of the government's three letter agencies and DOD contractors. These facilities were established across the U.S. to provide the joint reserve community with the ability to train and fight in a regional facility so they could provide direct support at a considerable savings to the government.

After learning more about the JRICs, I knew I had a possible solution to the JFCOM problem: take JRIC's capability and Reserve personnel and bring them together at JFCOM's JTF mission rehearsals.

Joint Solution, Everyone Wins

DIA was able to bring reservists to a JRIC close to the reservists' home station, saving the per diem and travel costs associated with normal Reserve missions. For example, a Dallas/Fort Worth reservist was called to duty for 30 days at the JRIC there in support of the Iraq mission. As a result of the JRIC's capabilities, he was able to remotely complete all mission requirements for the JFCOM Iraq mission rehearsal; and it was indistinguishable to JFCOM that the DIA support was 2,000 miles away.

The savings in per diem, rental car and plane tickets totaled

\$6,500. Multiply that by about eight, 12-day events conducted annually at JFCOM with two to four reservists for each of these and the savings potential is great.

Reserve Support is a Must

DIA Reserve support to JFCOM joint training is attainable and ready. JRICs provide the capability and the mission that DOD should embrace. As for DIA at JFCOM, we are continuing to seek ways to leverage the JRIC's potential in order to better meet the warfighter's needs in preparation for deployment.

There are challenges in finding the ideal reservist for the right location, and this does not work for all requirements. However, DIA Reserve support has shown, once again, with a little coordination and staff planning, how critical they truly are to the success of our men and women defending this great nation. ☛

What Sparks Your COMPASSION?

By Malinda D. Worley, DA

This year's Combined Federal Campaign is hoping to go green and grow in participation. The campaign has something for every interest and every budget.



For many federal employees, the Combined Federal Campaign (CFC) comes around each year as regularly as the leaves turn red and orange in the fall. However, this year might be a little different. Times are tough, and people are cutting back. But Jim Manzelmann, deputy director for Mission Services (DA) and the vice chairman of the agency's 2009 campaign, is confident that DIA employees will come through.

"Charities need our support now more than ever," Manzelmann said. "The amount doesn't matter, over

the year it adds up. You're going to make a difference."

Making a difference is what this campaign is all about. CFC has been collecting money for various charities — now more than 5,000 — since 1961, and DIA has been there since the beginning. CFC vets the charities before they can be included in the program, and all employees can be confident their contribution is going fully to the charity they select.

"All money pledged goes to the employee's choice; there is no

percentage siphoned off to the CFC organization," Bill Olexy, CFC deputy campaign manager, said. "The Office of Personnel Management pays a flat fee out of their annual budget to support the campaign. DIA employees can be confident that whatever they choose to donate goes right to that charity."

Olexy is part of the DIA campaign committee organizing this year's programming and was the principal sponsor of selecting DIA's theme: "Compassion." Although the campaign touts the weekly

Photo by Margan C. Kerwin, CP



Vivian Turnbull, vice deputy director for Mission Services, pulls up the online CFC catalog.

dollar totals, the committee wants to focus on where the money is going and what the money is doing.

"The outward appearance of the campaign is about money, but the money is only the vehicle to support the work of the charities. Contributing to CFC shows what sparks your compassion," said Olexy.

Manzelmann echoes Olexy's comments, saying, "Compassion is the prime reason people give to anything. You want to make a difference, whatever you believe in."

Another focus of the campaign this year is raising the level of

how much you contribute. Take what you spend one day on coffee and pledge that amount every week. Everyone can find something that fits in with their values or interests."

And there's something for every budget too — with payroll deduction you can pledge a single dollar every pay period if you choose.

"Spreading your donation over the entire year makes it possible for us to give even more," says DIA Campaign Manager James Berry. "It's tough to write a check for \$50, but if I give \$2 every pay period, it's about the same thing."

participation. Although DIA has consistently exceeded its financial goals, participation has been less than 50 percent. In 2008 the campaign raised more than \$1.4 million for charities, but participation was just under 32 percent.

"This year I'd like to increase participation as much as possible," Manzelmann said.

"It doesn't matter

Another aspect of this year's campaign that Manzelmann likes is the effort to be more environmentally friendly. The national campaign now has both the catalog and the pledge form online, and DIA employees have access to both via JWICS or SIPRNet. The Catalog of Caring is searchable, so you can more easily find the charities you'd like to support. And although hard copies of the catalog are available, each federal entity received fewer this year, so employees are encouraged to review it online.

Advertising for campaign events is also taking an environmentally friendly approach. Signs are produced with biodegradable materials or by recycling existing posters. Keyworkers are using the master calendars posted in common areas or the CFC Web site to advertise their events.

Manzelmann says he enjoys the fun and enthusiasm of the directorate events, and he's always ready to talk to groups about CFC and how good it feels to give. "The people who benefit from CFC aren't far away, they're right here in our community — sometimes they're your co-workers. You can see the compassion all around you. It's a rewarding feeling knowing you made a difference in someone's life." ➔

Who Said INTROVERTED Was a Bad Thing?

By Lynn "Ann" Griffith, CS

Introvert? Extrovert? Somewhere in between? This month's Knowledge Lab book review looks at the benefits of both and how to bring them together in the workplace.

The book "The Introvert Advantage: How to Thrive in an Extrovert World," by Dr. Marti Olsen Laney, provides insight and practical, concrete advice to people who work in organizations like DIA that "think for a living."

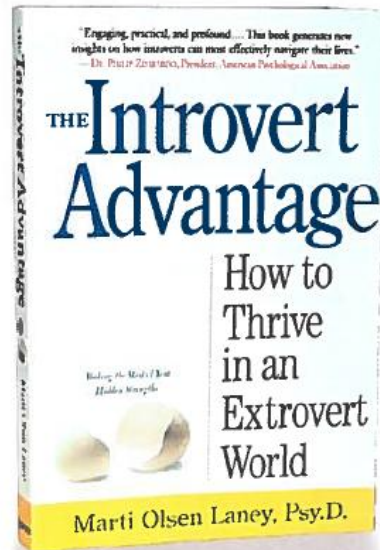
We commonly view introversion as associated solely with personality. Introverts are tagged as shy, quiet or uneasy in groups. Such views of introverts are reinforced quite naturally because 75 percent of people in the world are extroverts. Many intelligence professionals believe that analysts are largely introverts.

But what does it really mean to be introverted or extroverted? Laney says that due to unique brain physiology, introverts and extroverts generate and use energy differently, communicate differently, and have different thinking strengths. These key differences can cause confusion when working together.

- **Energy:** Extroverts feed off of other people to be energized. Introverts are drained by interaction and require quiet time to refill drained reserves.
- **Communications:** Extroverts think and talk simultaneously. Introverts are just the opposite; they operate sequentially needing time to formulate ideas before speaking, a behavior often seen in meetings of analysts. Introverts may stay quiet or speak tentatively during discussion of new ideas, possibly leading extroverts to think they are passive or not team players.
- **Thinking:** Extroverts think off the top of their heads. Introverts think in an ongoing dialogue with themselves, comparing old and new experiences. They excel at reflection, which is another reason to believe most analysts are introverts.

In the section on workplace relationships, Laney provides key insights into special talents introverts and extroverts contribute to teamwork, as well as what they each need to work most efficiently. For example, introverts like to work long complex problems, have good attention to detail, need to think and reflect before speaking and acting, work alone contentedly, and need little supervision. Extroverts become impatient or bored when the work is slow or repetitive, respond quickly to requests and can act without much advance thinking, like to be part of the majority opinion, and feel isolated without management support.

Laney says that understanding each other's styles helps introverts and extroverts maximize individual talents while contributing to the best outcome. Here is an example. Extroverts excel at



Title: The Introvert Advantage: How to Thrive in an Extrovert World

Author: Dr. Marti Olsen Laney

Published in 2002 by Workman Publishing Company

Laney is a researcher, educator, author and psychotherapist specializing in introversion.

brainstorming. To reduce pressure on their deep-thinking introverted colleagues while ensuring all voices are heard, teams can consider having two brainstorming sessions. In session one, all ideas will be considered, absolutely no criticism will be permitted, and some people will just listen and provide their input the next day. At session two, all ideas can be grouped into themes

and prioritized, results will be discussed, and solutions and alternative selected. By using this two-session approach, the talents of both groups are tapped; extroverts contribute spontaneously, and introverts have additional thinking time to prepare and articulate ideas.

Finally, Laney addresses how to deal with bosses who are introverted. Introverted bosses can have excellent leadership qualities like integrity, good judgment, intellectual curiosity, and the ability to look at the past, present and future, just to name a few. However, they may forget to communicate expectations, have trouble delegating, or not realize the importance of praise or rewarding good work. Laney recommends that the introvert boss discuss expectations and put them in writing, ask their staff for feedback, and give their employees feedback on strengths and weaknesses.

As an introvert myself, reading "The Introvert Advantage" was a wonderful experience. In a light-hearted, readable style, Laney holds up a mirror for introverts, debunking the myth that we are flawed personalities. Instead, she provides real-life examples, concrete advice and tips that have helped me examine how I can contribute my best ideas. This book is a recommended read for both introverts and extroverts to better understand the relationships that impact all areas of our lives, as workplace colleagues, friends, partners and family members.

The Knowledge Lab purchased 30 copies of "The Introvert Advantage" for DIA civilian or military employees for their professional development. If you are interested in borrowing a copy, please contact Ann Griffith at (202) 231-4008. ☛

Post of the Month: U.S. Defense Attaché Office TBILISI

By the Directorate for Human Intelligence, DH

Country History

The region of present-day Georgia has been continuously inhabited since the Stone Age. Throughout its early history, Georgia was controlled by a series of foreign occupiers including the Romans, Persians, Arabs and Turks. Georgia was incorporated into the Russian empire in the early 19th century and remained so until the Russian Revolution of 1917. Independent from 1918 to 1921, Georgia was forcibly incorporated into the USSR until the Soviet Union dissolved in 1991.

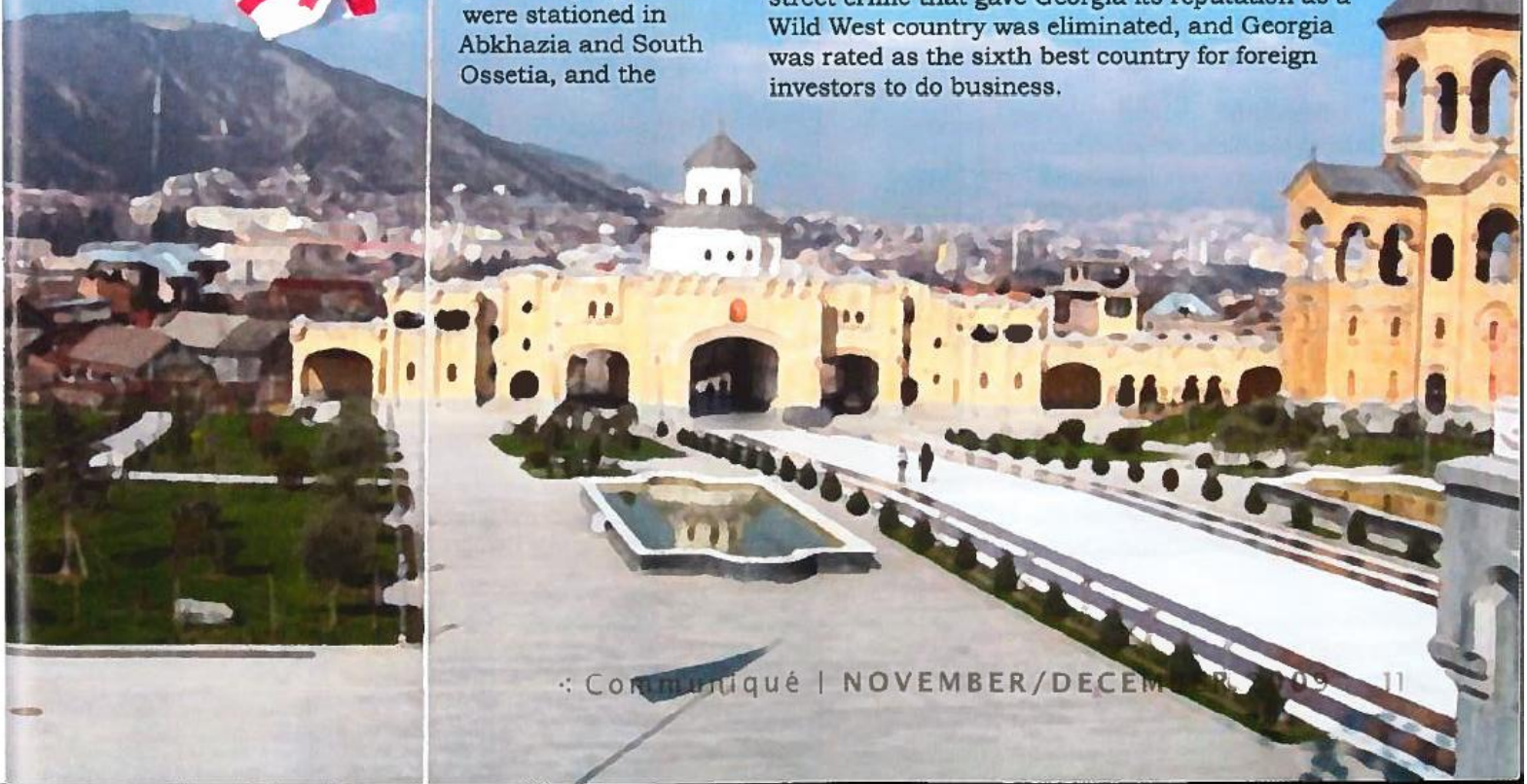
During the interim years of 1991-2003, civil wars fractured the Georgian state into four parts: greater Georgia and the separatist regions of Adjara, Abkhazia and South Ossetia. Then-President Eduard Shevardnadze felt compelled to enter the Commonwealth of Independent States to gain

support from the Russian Federation to stop the shooting in all three separatist regions. As a result, so-called Russian peacekeeping forces were stationed in Abkhazia and South Ossetia, and the



Russian-backed crime lord Aslan Abashidze controlled Adjara. This period is considered "lost years" in terms of development in Georgia as organized crime, corruption and failing infrastructure characterized daily life. It seemed as if Georgia would go the way of Somalia and Afghanistan and become the first failed state in Europe in the new century.

An attempt by the incumbent Georgian government to manipulate national legislative elections in 2003 touched off widespread protests — the Rose Revolution — and led to the resignation of Shevardnadze. New elections in 2004 swept Mikheil Saakashvili into power along with his National Movement Party, and began the renaissance of the Georgian state. While Abkhazia and South Ossetia remained out of Georgian governmental control, the new government succeeded in ousting Abashidze from Adjara, leading to the development of the city of Batumi as the premier beach resort on the eastern coast of the Black Sea. The Saakashvili government made wide-sweeping reforms that virtually eliminated petty corruption; improved roads, water and electricity delivery; and brought the Internet into Georgian homes. By 2007 the street crime that gave Georgia its reputation as a Wild West country was eliminated, and Georgia was rated as the sixth best country for foreign investors to do business.



Location: Tbilisi, Georgia

Population: 4.6 million (July 2009 estimate)

Language: Georgian (official), Russian, Armenian, Azeri

Ethnic groups: Georgian, Azeri, Armenian, Russian

Basic Greeting: "Gamarjoba" (phonetic) = "Hello"

After a series of Russian and separatist provocations in summer 2008, Georgian military action in South Ossetia in early August led to a Russian military response that not only occupied the remaining separatist areas, but large portions of Georgia proper as well. Russian troops pulled back from most occupied Georgian territory, but in late August Russia unilaterally recognized the independence of South Ossetia and Abkhazia where it maintains a physical and military presence to this date. The Russian Federation still maintains five U.S. Humvees they stole from the port of debarkation during this conflict, calling them "war trophies." It is safe to say that Georgia's relations with its northern neighbor play a major role in the life of all Georgian citizens and the U.S. Defense Attaché Office (USDAO) Tbilisi.

Host Country Highlights:

Following the Rose Revolution, a series of reforms was launched to strengthen the country's military and economic capabilities. In a recent speech to Parliament, Saakashvili focused on five broad areas for reform in the next several months: elections, constitutional revisions, judicial independence, media and national security cooperation.

The Georgian Ministry of Defense (MOD) is currently undergoing reforms to professionalize the

military force. These reforms include doctrine development, professional military education and force restructuring. As part of these "quality over quantity" reforms, career progression tracks are being instituted similar in nature to those of the U.S. military, though this is proving to be difficult in the current Georgian military culture where rank is not necessarily as important as title or position. Though significant progress has been made thus far, the August 2008 conflict with Russia, the international financial crisis and the current restructuring efforts are having a direct effect on the MOD's budget flexibility. On a positive note, in June, Georgia agreed to send a battalion to support the International Security Assistance Force mission in Afghanistan. Georgia previously supported Operation Enduring Freedom with approximately 2,000 personnel, though a significant portion was redeployed to Georgia in response

to the Russian invasion of South Ossetia.

Overall, U.S.-Georgian relations are excellent and are continuing to improve.

Operational Highlights:

The USDAO in Tbilisi is tasked with representing the secretary of defense, the secretaries of the armed services, the chairman of the Joint Chiefs of Staff and the

USDAO Tbilisi attachés LtCol John Thurman, left, and COL Matthew Brand, center, welcome Commandant of the Marine Corps Gen James Conway at the Tbilisi airport.



Photo by Cpl Erin Kirk-Cuomo



USDAO Tbilisi attachés COL Matthew Brand, second from left, and LTC Michael Varuolo, far right, at the Orpolo Live Fire Demonstration in July 2009.

Photo by Turkish ALUSNA Capt. Murat Yilmazarslan

director of DIA. USDAO Tbilisi also provides political-military advice to the ambassador. All attachés enjoy very stable and cooperative relations with Georgian military and political officials.

The four-person DAO in Tbilisi was awarded the National Intelligence Meritorious Unit Citation for their coverage of the Russia-Georgia conflict of 2008. USDAO Tbilisi played a critical role in support of the intelligence community, the national policymaking community and the Department of Defense by providing valuable information and critical insight in the volatile state of affairs throughout the duration of the conflict.

This past July USDAO Tbilisi attachés attended the first Georgian live-fire exercise since 2007. The tactical scenario for the event consisted of a battalion in a deliberate defense facing a much larger attacking adversary. The tactical situation was phased to replicate various events that might occur during such a situation. ☛



Photo by Goga Iosebldze

USDAO Tbilisi OPSNCO SFC Christopher Culling, center, and MSgt Duane Auguston, left, speak with a U.S. Embassy expediter.

Language Technology AT YOUR FINGERTIPS

By Nicholas A. Bemish and Dr. Jennifer A. DeCamp, HC

The Language Technology Resource Center provides tools and applications to help analysts and translators find the right technologies to accomplish their mission.

DIA is continually trying to make the best technology solutions available to its work force. The Directorate for Human Capital's Foreign Language Management Office (HC-FL) is doing their part by teaming up with several other intelligence community (IC) agencies to provide a resource where program managers can obtain up-to-date information on various language technologies.

The Language Technology Resource Center (LTRC) Web site provides information on a broad range of language products and tools. It also includes an online survey for product developers and researchers that will provide the U.S. government and the public with information about their work. The site is available on Intelink on NIPRNet, SIPRNet and JWICS. The version of Intelink on NIPRNet is available through Army Knowledge Online.

The LTRC has SharePoint sites for government communities of interest, which include translator working groups, an interpreters working group and users of the National Security Agency's (NSA's) Wordscape, an NSA-developed language dictionary look-up tool. Translator working group sites are set up for Arabic, Chinese, Dari, Farsi and Russian, although more can be added easily with a request to HC-FL.

Each translator working group site also includes a terminology blog, where translators can tap the expertise of their colleagues across the IC on the meaning or evolving meaning of terms. This also can provide a closer link between translators and analysts for collaboration on content that may be technically challenging or specific to a particular topic of interest. The plan is to link the discussions to terms in Wordscape

to capture more information about the terms.

This site has the potential to be a valuable tool for the IC and program managers interested in learning which tools are either ready for integration into enterprise solutions or are being researched and developed for future integration. DoDIIS portfolio programs, like TripWire Analytic Capability and A-Space, that have identified language tool development in their capability design documents can benefit from this site in determining future systems that may meet their existing program requirements. Task force members who are focused on a region or "hot spot" that has limited human language capacity can use this site to determine critical gaps or near-term solutions for immediate collection results. The possibilities are only left to the imagination of the user.

Reports can also be generated from the tools database. The most common report is a particular language crossed with a particular application, for example, Arabic

crossed with optical character recognition.

A separate search capability is provided for dictionaries in order to capture the many types of tools available. A standard dictionary search includes

dictionary type, source language, target language, domain, register and year of publication. A software comparison capability — currently in prototype — will allow users to select the type of technology and the language or dialect. Users can then select from a list of requirements and the system will rank products in the database according to their selections.

A further report can provide information on future products in a particular language and technology type. This information is important for many organizations, as it may influence decisions to acquire software or to wait for new products. The tools section of the LTRC includes links to online machine translation tools that can be used by linguists and analysts.

Public information is also provided on conferences, general announcements, new technology and standards. Government personnel logging in to the LTRC can also see government-only information. Public information is provided on professional organizations and resources, and on community standard practices.

To find the LTRC Web site on JWICS, go to <http://firc.inscom.ic.gov/>.

The Art of FOREIGN DISCLOSURE

By Charles L. Shoemaker, IE

DIA's foreign disclosure officers protect sensitive sources and methods while providing vital intelligence information to international partners.

DIA is the executive agent for a specific category of classified military information, namely military intelligence. According to the Department of Defense National Disclosure Policy, military intelligence is defined as "information of a military character pertaining to foreign nations and areas."

The responsibility for foreign disclosure is one that is not to be taken lightly, and DIA has

developed and implemented a formal training program for foreign disclosure officers (FDOs) focused on military intelligence. DIA trained 500 intelligence professionals across the Department of Defense on the aspects of release and disclosure of military intelligence during the last fiscal year. Training is vital to sensitize FDOs to the need for the protection of sources and methods when exercising their delegated authority to provide classified

information to foreign partners or multinational organizations. DIA's FDOs represent the front line of defense in protecting sensitive sources and methods in the production of DIA intelligence that is ultimately used to support operations. DIA FDOs work closely with their counterparts in the combatant commands and the services.

What is a DIA FDO?

DIA FDOs are a cadre of intelligence professionals who are responsible for the review and release of DIA products or information. They are found in every production element in the agency, and may even be sitting in the cubicle next to you. FDOs support

the role DIA plays in providing military intelligence as part of ongoing relationships with various foreign partners and multinational organizations. The role of an FDO has become more prominent as the U.S. increasingly works in a coalition environment to achieve its goals as part of the international community.

An Emerging Role

The increased need for trained foreign disclosure professionals can be seen most clearly within existing and emerging coalition operations in which the U.S. is either the lead or a significant member. The wide variety of rules, guidance and policy regarding national security information requires a firm grounding in how



intelligence is produced and used, as well as a sense of the evolving nature of intelligence. Training provides a basic view of the art

of foreign disclosure, but training alone cannot anticipate the changing intelligence landscape in which DIA operates. Providing all-source intelligence, while protecting sources and methods, is a daily challenge and an important responsibility. As the final authority on the sharing of military intelligence with our multiple foreign partners and multinational organizations, DIA's FDO community fills a vital role in a crisis-dominated intelligence environment. ♦

Editor's note: The author is the senior disclosure intelligence officer in the Office of International Engagement (IE) and is the training instructor for DIA's disclosure courses.

FE's Internal Controls Branch HELPS to SAFEGUARD DIA

By the Internal Controls Branch, FE

The Office of the Chief Financial Executive does its part to guarantee DIA's assets are protected by ensuring the agency is in compliance with the Federal Managers' Financial Integrity Act.

The Office of the Comptroller Internal Controls Branch (FE-2/FE-2C-1) helps DIA protect whatever it has or does, ensuring the integrity of DIA processes, protection of DIA assets and compliance with the Federal Managers' Financial Integrity Act (FMFIA).

FMFIA is one way Congress exercises its responsibility to control the activities of federal enterprises. It directs the head of each agency to determine whether its resources are adequately protected and its business processes have integrity, and to certify annually to Congress and the president that the agency's activities are being managed and are under control.

While the FMFIA itself is less than two pages, the breadth of what it requires the director to certify is enormous. The director must make four assertions: that an evaluation of controls was accomplished, the controls are in place and are effective, and the following FMFIA objectives are being achieved:

- Laws and regulations are followed (doing what we are told).
- Programs achieve intended results and resources are protected from waste and mismanagement (doing it well).
- Reliable and timely information is reported and used for decision-making (reliably reporting how we do it).

“CONTROLS HELP ENSURE THAT THE PROCESS HAS INTEGRITY, AND BY PROVIDING INTEGRITY, WE SAFEGUARD OUR RESOURCES AND OUR NATION.”



The objectives are simple because they direct the agency to be a good manager, which involves five basic functions: planning, organizing, staffing, directing and controlling. Planning decides what is to be done. Organizing sets up a structure to carry out plans. Staffing selects personnel to accomplish

plans. Directing sets out the ways to accomplish plans, and controlling assesses how plans are being implemented.

Controls include any method to ensure that plans are being carried out. It involves any activity including policies, procedures, plans and even the very structure

of the organization. It is an integral part of managing, and is how the manager ensures that progress is being made toward achieving the objectives of the activity. Controls help ensure that the process has integrity, and by providing integrity, we safeguard our resources and our nation. ♦

PROTECTING DOD's Critical Infrastructure

By Jonathan Bonniwell, CE

DIA looks inward to develop a program that uses existing DIA resources to better protect the Department of Defense's critical infrastructure at home and abroad.

DIA's Office for Critical Infrastructure Protection and Homeland Defense (DDC) has begun a joint venture with the Directorate for Analysis' Defense Resources and Infrastructure Office (DI/DRI) to identify interdependencies of the intelligence sector's task critical assets (TCAs) and to provide reach-back support to U.S. Northern Command's (NORTHCOM's) Defense Support of Civil Authorities (DSCA) mission. DRI will use its existing network visualization tool, Functional Intelligence System of Hierarchical Networks (FISHNet), to capture, digitize, visualize and analyze interdependencies among intelligence sector TCAs.

This pilot, known as Monument Park, officially launched June 1.

There are a total of 10 sectors that were created by the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. The other sectors are finance, health, defense industrial base, space, logistics,

transportation, personnel, public works and the global information grid.

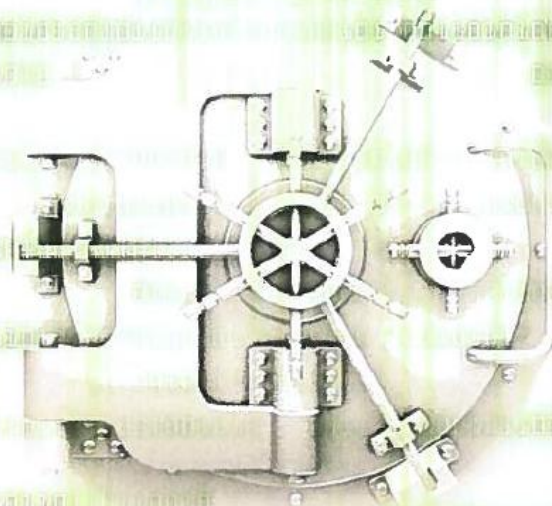
DIA was appointed as the defense infrastructure sector lead agent (DISLA) for the intelligence sector, which was delegated to DDC. As the lead for this sector for the Department of Defense (DOD), DIA must identify, prioritize and protect defense intelligence critical infrastructure that is essential to DOD mission execution.

Within these other sectors across the defense critical infrastructure community, there has been an effort to "geo-enable," or graphically represent, all available assets to be able to conduct interdependency analysis. Instead of building a database and geospatial information system from scratch as other sectors have done, DDC looked within DIA to see what capabilities the agency already possessed, and how to best use these capabilities to conduct interdependency analysis.

The Modernized Integrated Database (MIDB) was already a database storing military data on foreign assets, and is widely used around the globe by DIA and its customers. FISHNet was already being used to geospatially display data from MIDB to conduct

various analytical studies. After working with General Counsel to ensure compliance with Executive Order 12333, MIDB will now be able to store data on U.S. government facilities and infrastructure.

Monument Park provides three full-time DRI analysts dedicated to identifying critical nodes and interdependencies. Initially, FISHNet will overlay the intelligence sector's TCA list while incorporating Homeland Security Information Program Gold Data and publicly available commercial data. This information will be stored in a separate database in accordance with a concept of operations approved by General



Counsel. This data will be transformed into the FISHNet schema by DRI analysts and will be used to conduct an initial interdependency analysis of the intelligence sector's TCAs within the National Capital Region, including the transportation and logistics networks, electric power lines, communications networks, and fuel and natural gas pipelines on which these assets depend.

DRI analysts will ultimately apply their expertise in conducting interdependency analysis on foreign assets to Monument Park. Results from this initial project lay the foundation for the analytic trade-craft in conducting interdependency analysis of U.S. defense critical infrastructure.

The project will also provide DRI analysts a robust foundation to conduct modeling and simulation using tools developed within the Sudden Capital program in order to determine the cascading effects of failures, including those from natural disasters or other significant events. This analysis will provide DOD and government policymakers with the prescriptive intelligence edge they will need to assess impending threats and hazards. It will also support NORTHCOM's DSCA mission and potentially state,

local and tribal first responders. The ultimate goal of this initiative will be to support asset owners in making risk response decisions on identified TCAs in accordance with the DOD Instruction 3020.45, Defense Critical Infrastructure Program (DCIP) Management, from April 21, 2008.

Follow-on work will include translating the intelligence sector's current database, the Integrated Prioritized Asset Database (iPAD), into MIDB to begin a more robust interdependency analysis on DOD's intelligence assets. Activation of MIDB for U.S. data on DOD facilities and related infrastructure will enable it to serve as a repository for data collection, maintenance and dissemination to support analysis on DOD critical infrastructure assets, DOD critical infrastructure networks, critical nodes and post-event damage assessments. It will also allow for a "coalition of the willing" to transfer their data from disparate databases into one centralized location and take advantage of a mature, robust and stable database. ArcGIS users will also be able to pull data from MIDB for analysis. Greater collaboration will support national and DOD policy decision-making, as well as offer a means to improve DIA's support to homeland defense mission. *

CIO TIPS

Your monthly DS communications source for:

- Technology Tips
- DS Information and News
- IT Products and Services Highlights

JWICS - http://www.dia.ic.gov/admin/ds/communications/cio_tips/cio_tips.html

SIPR - <http://www.dia.smil.mil/admin/ds/index.htm>

Have suggestions or ideas?

Send an e-mail to CIO-TIPS on JWICS or SIPRNet ::::

The objectives are simple because they direct the agency to be a good manager, which involves five basic functions: planning, organizing, staffing, directing and controlling. Planning decides what is to be done. Organizing sets up a structure to carry out plans. Staffing selects personnel to accomplish

plans. Directing sets out the ways to accomplish plans, and controlling assesses how plans are being implemented.

Controls include any method to ensure that plans are being carried out. It involves any activity including policies, procedures, plans and even the very structure

of the organization. It is an integral part of managing, and is how the manager ensures that progress is being made toward achieving the objectives of the activity. Controls help ensure that the process has integrity, and by providing integrity, we safeguard our resources and our nation. ➤

PROTECTING DOD's Critical Infrastructure

By Jonathan Bonniwell, CE

DIA looks inward to develop a program that uses existing DIA resources to better protect the Department of Defense's critical infrastructure at home and abroad.

DIA's Office for Critical Infrastructure Protection and Homeland Defense (DDC) has begun a joint venture with the Directorate for Analysis' Defense Resources and Infrastructure Office (DI/DRI) to identify interdependencies of the intelligence sector's task critical assets (TCAs) and to provide reach-back support to U.S. Northern Command's (NORTHCOM's) Defense Support of Civil Authorities (DSCA) mission. DRI will use its existing network visualization tool, Functional Intelligence System of Hierarchical Networks (FISHNet), to capture, digitize, visualize and analyze interdependencies among intelligence sector TCAs.

This pilot, known as Monument Park, officially launched June 1.

There are a total of 10 sectors that were created by the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. The other sectors are finance, health, defense industrial base, space, logistics,

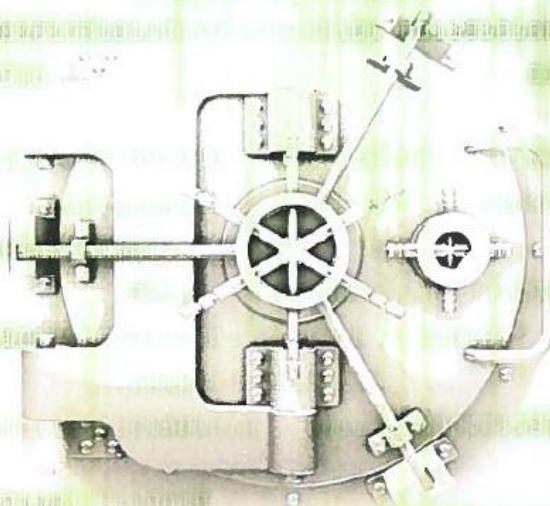
transportation, personnel, public works and the global information grid. DIA was appointed as the defense infrastructure sector lead agent (DISLA) for the intelligence sector, which was delegated to DDC. As the lead for this sector for the Department of Defense (DOD), DIA must identify, prioritize and protect defense intelligence critical infrastructure that is essential to DOD mission execution.

Within these other sectors across the defense critical infrastructure community, there has been an effort to "geo-enable," or graphically represent, all available assets to be able to conduct interdependency analysis. Instead of building a database and geospatial information system from scratch as other sectors have done, DDC looked within DIA to see what capabilities the agency already possessed, and how to best use these capabilities to conduct interdependency analysis.

The Modernized Integrated Database (MIDB) was already a database storing military data on foreign assets, and is widely used around the globe by DIA and its customers. FISHNet was already being used to geospatially display data from MIDB to conduct

various analytical studies. After working with General Counsel to ensure compliance with Executive Order 12333, MIDB will now be able to store data on U.S. government facilities and infrastructure.

Monument Park provides three full-time DRI analysts dedicated to identifying critical nodes and interdependencies. Initially, FISHNet will overlay the intelligence sector's TCA list while incorporating Homeland Security Information Program Gold Data and publicly available commercial data. This information will be stored in a separate database in accordance with a concept of operations approved by General



Counsel. This data will be transformed into the FISHNet schema by DRI analysts and will be used to conduct an initial interdependency analysis of the intelligence sector's TCAs within the National Capital Region, including the transportation and logistics networks, electric power lines, communications networks, and fuel and natural gas pipelines on which these assets depend.

DRI analysts will ultimately apply their expertise in conducting interdependency analysis on foreign assets to Monument Park. Results from this initial project lay the foundation for the analytic trade-craft in conducting interdependency analysis of U.S. defense critical infrastructure.

The project will also provide DRI analysts a robust foundation to conduct modeling and simulation using tools developed within the Sudden Capital program in order to determine the cascading effects of failures, including those from natural disasters or other significant events. This analysis will provide DOD and government policymakers with the prescriptive intelligence edge they will need to assess impending threats and hazards. It will also support NORTHCOM's DSCA mission and potentially state,

local and tribal first responders. The ultimate goal of this initiative will be to support asset owners in making risk response decisions on identified TCAs in accordance with the DOD Instruction 3020.45, Defense Critical Infrastructure Program (DCIP) Management, from April 21, 2008.

Follow-on work will include translating the intelligence sector's current database, the Integrated Prioritized Asset Database (iPAD), into MIDB to begin a more robust interdependency analysis on DOD's intelligence assets. Activation of MIDB for U.S. data on DOD facilities and related infrastructure will enable it to serve as a repository for data collection, maintenance and dissemination to support analysis on DOD critical infrastructure assets, DOD critical infrastructure networks, critical nodes and post-event damage assessments. It will also allow for a "coalition of the willing" to transfer their data from disparate databases into one centralized location and take advantage of a mature, robust and stable database. ArcGIS users will also be able to pull data from MIDB for analysis. Greater collaboration will support national and DOD policy decision-making, as well as offer a means to improve DIA's support to homeland defense mission. ➤

CIO TIPS

Your monthly DS communications source for:

- Technology Tips
- DS Information and News
- IT Products and Services Highlights

JWICS - http://www.dia.ic.gov/admin/ds/communications/cio_tips/cio_tips.html

SIPR - <http://www.dia.smil.mil/admin/ds/index.htm>

Have suggestions or ideas?

Send an e-mail to CIO-TIPS on JWICS or SIPRNet ::::

Interview with Timothy C. McNeil Chief of the COUNTERINTELLIGENCE and SECURITY Office

By the Communiqué Staff, CP

The Communiqué staff interviewed Timothy C. McNeil, chief of the Counterintelligence and Security Office in the Directorate for Mission Services (DA/DAC), to discuss DAC's many missions, their role in safeguarding the agency and the intelligence community, and their plans for the future.

He assumed his current position in May 2009 and manages the agency's counterintelligence, security, antiterrorism, force protection, personnel security and law enforcement services programs. McNeil has 36 years of intelligence experience as an operator, analyst and planner serving at the operational, combatant command, joint staff and combat support agency levels, including 18 years at DIA. Prior to his position with DAC, McNeil served as DIA's deputy chief of staff.

COMMUNIQUE: Now that you've had time to become accustomed to DAC, what do you see as the organization's top three priorities in the near term? Far term?

MR. McNEIL: Our top priority for both the near term and the far term is the "insider threat," which I'll expand upon later. That's either a primary or secondary responsibility for every element of DAC. A second priority is to push support forward to DIA elements that are in the field — the deployed forces and human intelligence operations around the world. This is something that DAC has been doing a pretty good job of well before I



Photo by Daneta G. Billau, DA

Tim McNeil, chief of DAC, sat down with Margan Kerwin from Internal Communications to talk about DAC's priorities for the upcoming year.

arrived, but it's worth re-emphasizing its importance. A third near-term priority is updating our security policy documents. For example, our "Personnel Security Program" issuance is dated June 1995, and our "Information Security Program" issuance is dated 1993. Those two have now been updated, polished and submitted for approval by the chief of staff. We are working hard to put

thoughtful, coherent and updated security policies in the hands of our work force.

Looking longer term, there are priority issues across the board. We need to increase our technical surveillance countermeasures services in the most sensitive facilities within DIA. We have a limited number of polygraph examiners and need to make sure

we're applying that capability in a highly focused manner. We need to review our whole business plan for accrediting the thousands of SCIFs for which we are responsible. We have a relatively new cyber counterintelligence capability that we need to grow and develop with highly trained and motivated cyber warriors. In today's environment, information can be sent around the world in a nanosecond. We need to make sure this information is protected and received by trusted employees and not our adversaries — protecting critical intelligence information is vital to protecting our fighting forces. We also need to increase the manning level of our DIA Police Force, and reduce our emphasis on armed contract security personnel and contractor K-9 capabilities.

Because what this organization does is so important, we can never allow ourselves to become complacent, and we must strive to improve in every area.

COMMUNIQUE: *How do you envision DAC increasing support out to the field?*

MR. McNEIL: Moving support out to the field covers all of our mission areas. We have people deployed, and we send our employees out to support security forces around the world. We're regularly deploying our work force to conduct physical security, technical security, and anti-terrorism and force protection. For example, we send polygraph examiners to assist the Directorate for Human Intelligence (DH) when they're in the field, and review assessments of construction security plans and architectural drawings for their facilities. We try to push support forward, and recognize the special needs of the people that are a long way from headquarters and focus on them. Sometimes there's no substitute to getting a person on the ground in the field.

"Protecting critical intelligence information is vital to protecting our fighting forces."

There is also our reach-back capability. A lot of our support is having the expert capability here at headquarters so that if people in the field have security issues, they can come back and get answers to their questions.

DIA Police officers monitor the turnstiles in the DIAC Expansion to help employees with badge and access issues.



Photos by Margan C. Kerwin, CP



A DIA employee is suited with an arm cuff in preparation for a polygraph exam.

COMMUNIQUE: *What should the work force know about DAC that they don't already know?*

MR. McNEIL: The director has broad responsibilities and authorities that go beyond DIA, and DAC executes a number of those on his behalf. For example, DAC accredits 3,500 SCIFs in the National Capital Region, throughout CONUS and around the world. DAC determines security clearance eligibility and grants clearances to personnel in the Office of the Secretary of Defense; the Joint Staff; Department of Defense field activities; the White House Communications Agency; the White House Military Office; and all of the defense agencies except for the National Reconnaissance Office, the National Security Agency and the National Geospatial-Intelligence Agency. When it comes to security clearances, we have a total service population in excess of 75,000. Another example would be the direction and oversight of the Defense Special Security System, to include promulgation of appropriate security policies and procedures.

COMMUNIQUE: *What is the insider threat and why is it such a concern?*

MR. McNEIL: The insider threat is when we have someone we've granted a security clearance and access to



DIA Police Officers David Fuller and Kevin Dewyngaert monitor the control boards in the Law Enforcement Operations Center in the DIAC. All DIA Police actions and dispatches go through this center.

our most sensitive systems and that person betrays the nation's trust and confidence. When I first came into the intelligence business 36 years ago, I had access to a four-drawer security container filled with classified documents, and that was about it. Now with JWICS, all of our employees have extraordinary access, and the potential damage that a betrayal could cause is so much more than it was in the days when I first came in. Every intelligence agency has been penetrated at some point, and that includes DIA.

We are working across the entire DAC organization and all of the different areas to tie the security effort together in a unified way to focus on the insider threat. We cannot afford to be complacent. One way employees can help us combat this threat is to report suspicious activities. Maybe it will be nothing, and that's fine. But that's typically one of the ways these things are discovered: it's a diligent employee that sees something that doesn't seem quite right, and they tell someone about it.

respect for our employees and how they're treated during this process. We know that a polygraph examination is intrusive, and, frequently,

COMMUNIQUÉ: *Polygraph exams are always a source of unease and consternation, whether it's an employee's first or fifth test. What can you tell us about the polygraph process, and what can employees do to better prepare themselves for their polygraph?*

MR. McNEIL: Our polygraph examiners are the best in the business, and we have great

attempt to defeat the examination. These efforts are typically very crude and easily detectable. It's not helpful, and there are consequences to those sorts of actions that we would all like to avoid.

COMMUNIQUÉ: *We see the DIA Police Force behind the counter in the DIAC lobby — tell us more about their mission.*

MR. McNEIL: We're very proud of our DIA Police Force. All of our police officers are trained at the Federal Law Enforcement Training Center. Additionally, they are extensively trained in a broad range of emergency response capabilities, including medical emergencies; hazardous material handling; direct action; and chemical, biological and radiological contamination. They're doing a great job protecting our personnel, our facilities and our information.

"Sometimes there's no substitute to getting a person on the ground in the field."

very sensitive personal information will come out during the examination. People need to know that we protect that information rigorously and handle it on a "must know" basis. We conduct our program with the utmost integrity.

I do have a concern that we are seeing an increasing number of people who research polygraph examinations on the Internet and



“An alert work force is an essential component to our security.”

The DIA Police Force and their mission will also be expanding. The areas where we have armed contract security officers will convert to fully trained police officers over time. You have seen this in the DIAC already, and it will happen at our other facilities in the future. We are very excited about the quality of the men and women that we have been recruiting, and see everything headed in the right direction.

COMMUNIQUE: *From your point of view, how do we balance the need to share with need to know?*

MR. McNEIL: That's a real challenge. The traditional problem had been that certain intelligence agencies were not willing to share information with other intelligence agencies. Now we're getting into coalition warfare, and there are more and more cases of asking how we share information with allies that are in the fight with us. The terrorism threat requires us to share information with law enforcement organizations. For example, our police force has contacts in the law enforcement community, so we're able to leverage a lot of capabilities they have, but how much classified information are we able to share with local,

state and tribal law enforcement agencies? That's going to be a tremendous challenge. Sharing intelligence involves risk, and the decision of how much risk to accept is made by the director and not by his security organization.

COMMUNIQUE: *What can we do as employees to help make DIA safer?*

MR. McNEIL: DIA puts great trust in our employees, and with that trust comes the responsibility to follow the stringent rules of protecting classified information. The reason we need to follow these rules is not to avoid a security violation, but because we have the responsibility to protect sensitive information that could harm our national security if compromised. Our employees have the responsibility to report security violations. On a recent Friday evening, the phone rang and it was a distraught new DIA employee who had inadvertently taken some classified material out of the office. I told her to take the material to the nearest DIA facility to bring it back under appropriate government control, and to send me an e-mail on Monday morning reporting the incident. She did the right thing, and acted immediately and



Photos by Margan C. Kerwin, CP

Bo and his K-9 handler Kevin Collier inspect a vehicle entering the Clarendon parking facility.

responsibly to correct the mistake and report it. Security violations do happen from time to time, and we need to learn from them.

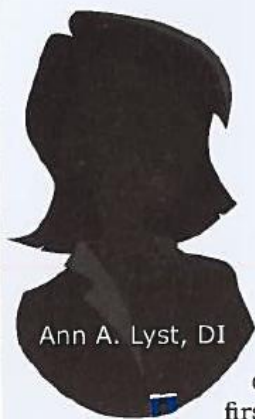
COMMUNIQUE: *Is there anything else you'd like to add?*

MR. McNEIL: I have mentioned our concerns about the insider threat, and would ask all our employees to report suspicious activity that they might observe to our Investigations Division for appropriate action. An alert work force is an essential component to our security. ☛

“We have the responsibility to protect sensitive information that could harm our national security if compromised.”

Safeguarding DIA: Twenty Years and Counting

By the CounterIntelligence and Security Office, DA



Ann A. Lyst, DI

As I sit here waiting for my final security retirement interview with DIA's Counterintelligence and Security Office (DAC), it seems like only yesterday I was first introduced to DAC and its mission to protect our agency's people, property and information. DAC works behind the scenes to keep DIA safe, no matter where in the world our mission takes us.

From new hire to deployment to retirement — and every day in between — DAC is there around the clock to safeguard DIA.

DIA Police Force: Trained and Ready to Help

As a new employee, you may have first met a DAC police officer directing you where to park, or at the visitor control kiosk when you entered the facility for the first time. DIA police officers are trained professionals ready to assist. Their training begins with a 13-week program at the Federal Law Enforcement Training Center and continues throughout their career. The DIA Police Force protects DIA all day, every day. Our officers are prepared to respond to fires, and many are also certified emergency medical technicians. Their ability to respond quickly has saved lives and property.

And it doesn't stop there. I'm amazed at the special training our police force has. In addition

to hazardous materials certified officers, we also have a Special Response Team. These officers are certified to respond to all critical incidents, such as hostage situations, standoffs and chemical, biological, radiological and nuclear (CBRN) situations.

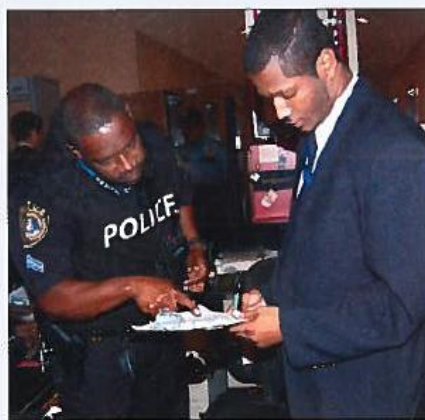
Did you know that our police force offers a self-defense course to all DIA employees? This two-day training prepared me to encounter an attacker. I learned about home defense planning, safe rooms, and safety and protection devices to protect me and my family.

The self-defense hands-on training was great fun, and at graduation we suited up in protective equipment — “Red Man gear” — for scenario-based training. This course is also provided to the spouses of our attachés, and recently helped one spouse protect herself and her family from an assailant.

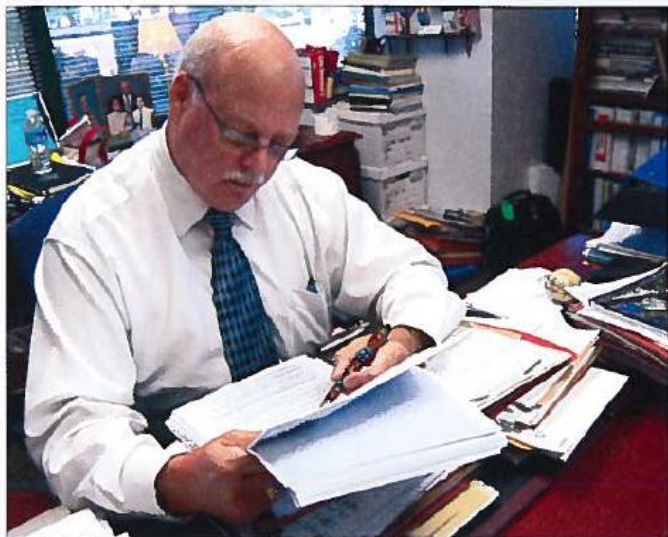
“People [at DIA] are responsible for many things, and we are the ones that protect them and enable them to do their job without worries or concerns,” said Lt. Anthony Simpson, one of the DIA Police training coordinators.

Around the clock at the DIAC, it is very nice to know all I have to do is call (202) 231-2725 and the DIA Police are there to help. Emergencies, crime, even an escort to my car or help with a dead battery — all you have to do is call. For DIA Police locations

DIA Police Officer Kevin Dewyngaert monitors the DIAC, other DIA locations and the news in the Law Enforcement Operations Center.



DIA Police Officer Bernard Bryant checks over a security log with Donnell Floyd at the Clarendon security kiosk.



Karl Glasbrenner, chief of the DAC Personnel Security Division, reviews an employee's SF-86. When you update your SF-86, remember to:

- ✓ Be honest in your dealings and information sharing.
- ✓ Learn what the adjudication standards mean.
- ✓ Realize you are responsible for your personal and financial behavior.
- ✓ Follow all security requirements.
- ✓ Report any and all security violations to DAC for investigation.

and contact information, consult the DAC pullout contact card, included in this issue.

SF-86: Your Security Life Story

Long before I stepped foot into DIA, I filled out a Standard Form 86 (SF-86) and wondered how all this information would be used for my security clearance. Little did I know I was already working with DAC and its Personnel Security Division. Like many new employees, I did not fully understand the importance of the SF-86, and how my past, present and future experiences would need to be updated over time. I'm glad I kept a copy!

Our security clearances establish a level of trustworthiness. Karl Glasbrenner, chief of the DAC Personnel Security Division, recently explained that his division "...enables trust by determining trustworthiness of all the employees, contractors, military personnel and visitors who come to our agency and need access to our systems or facilities."

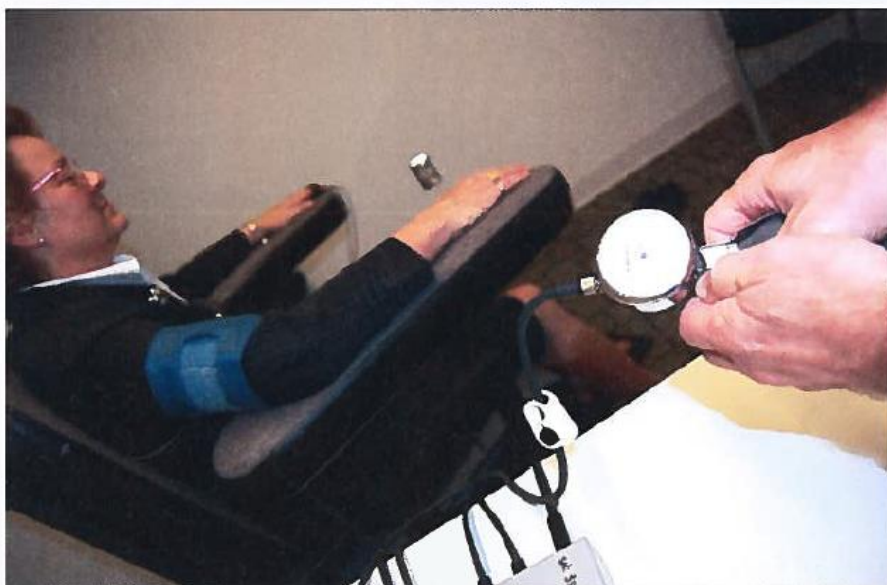
As you fill in your SF-86, resist the temptation to "forget" embarrassing past incidents, thinking the incident was so long ago that no one will care. It is much better to show you are trustworthy to follow security regulations, directives and requirements.

Assessing Your Credibility

Credibility assessment is one of several steps in processing a clearance. DAC's Credibility Assessment Program (CAP) acquires, develops and reports information leading to cogent and actionable intelligence via polygraph, interview and other trusted means. CAP's top priority is to support critical and time-sensitive operations and investigations that have the potential to impact human life, critical intelligence information and targets, or the viability of national security affairs. Examples are espionage

and other national security investigations, human intelligence (HUMINT) activities, offensive counterintelligence (CI) operations and warfighter support.

CAP provides worldwide polygraph and other credibility assessment services to DIA; the offices of the Director of National Intelligence (ODNI), Secretary of Defense and Joint Chiefs of Staff; combatant commands; joint task forces; and other federal agencies and Department of Defense (DOD) organizations. To perform its mission, CAP has traveled to 19 states and 22 countries on six



Every DIA employee must undergo a polygraph assessment.

Photos by Margan C. Kerwin, CP

continents, and CAP personnel have spent more than 2,200 days in a temporary duty or deployed status in the 2008 fiscal year.

CAP has embedded full-time support to the Global War on Terrorism for more than six years now. Within U.S. Central Command (CENTCOM), CAP has distinguished itself on numerous tactical and strategic HUMINT operations, foreign document and media exploitation, CENTCOM vetting initiatives, and unconventional wartime missions. Deployed examiners perform missions under extremely dangerous and austere conditions, and successfully evade threats jeopardizing lives and missions.

Since September 2005 all DIA positions are considered critical intelligence positions, so all applicants, military assignees, contractors and consultants have a periodic CI-scope polygraph

(CSP) test. CAP already gives pre-employment and initial screening to DIA and affiliates who have not been screened within three years of entering the agency. DIA CAP reciprocally accepts successfully completed CSP and expanded-scope examinations by other federal agencies.

If you follow and support DIA security requirements, taking a polygraph will be a breeze. The first part of the polygraph session is your opportunity to discuss any concerns. Use this time to clear up potential misunderstandings, and the rest of the test will go quickly. The entire exam takes about two to four hours, and some people return for a second session. Before your polygraph, be sure to take daily medication(s) and be well-rested.

For more information about polygraph examinations, please contact:

- DIAC — Room L143, Expansion Wing (202) 231-1313
- Clarendon — Room 710, Arlington, Va. (703) 907-1313
- Alexandria — Central Processing Support Center (CPSC), Alexandria, Va. (703) 664-2975

Judge, Jury and Adjudicator

Adjudication is the next step in the clearance process, which brings up many questions about the time it takes to grant an initial clearance, update or transfer a clearance from another agency. An experienced adjudicator has spent years identifying behaviors that reduce a person's level of trustworthiness. For example, some people don't realize

they can be impacted by visiting social networking sites such as Facebook or LinkedIn, but these activities could make you a target for people who collect information. Some risky behaviors could lead to someone losing their security clearance and being removed from DIA and the IC, so be aware of this risk. Here are some helpful hints for you to keep in mind:

- Keep your DIA badge in a safe place
- Lock up your personal electronic devices
- Pay your credit cards on time
- Report foreign contacts and travel
- Report suspicious activity
- Check bags for classified material before going home
- Follow information assurance and computer security requirements
- Know that DAC counterintelligence focuses on staff behavior and threats

As you continue your career, you will work with DAC personnel many times. You will have a five year reinvestigation and may have life-changing events or travel to "risky" places. During your career you might also work on a special project or program in DIA that uses different levels of clearances. Much of what we do is classified top secret, but you may also handle sensitive compartmented information (SCI), or, under special situations, work with special access programs (SAPs) with different classifications.

I do solemnly swear that I will support and defend the Constitution...



When starting out, most people are excited about working with classified intelligence for the first time. The most important activity in Gateway is taking your oath to protect and safeguard DIA people, property and information. DAC will always be there to guide and help you fulfill your oath. Reporting security issues is one of the most important ways you can help DAC protect DIA.



Photo by Margan C. Kerwin, CP
Security Technician Keshon Foote prepares Kia Williams' badge information.

DAC personnel help new hires with identification forms, getting a badge, signing a security indoctrination, and reading new hires on to their level of clearance. DAC will help you at the Badge Office to get different badges that come in handy: IC badge, Common Access Card (CAC), Pentagon badge and courier

badge. Remember to keep your badges, system access and parking decals up to date. Badges are like keys to the building, so if you lose yours, please contact the badge office right away.

In July 2005 DA established a full-service Customer Service Center at the DIAC for all of DIA's personnel security needs. The center is manned by the Case Management Branch to assist with personnel security clearance matters and policy questions. The Security Services Branch provides security briefings, debriefings, badge distribution, indoctrinations and passing clearances, Pentagon pass applications, and CACs. For Customer Service Center hours and locations, consult the DAC pullout contact card.

Toothbrush? Check. Defensive Travel Training? Check.

There are several mandatory security courses that you need to take as a DIA employee, such as DAC Security Awareness, Anti-Terrorism and Force Protection, Escape Mask or Hood, and Foreign Travel training. Gateway provides your initial training, but some of this you will do on your own annually.

Foreign travel, either official or unofficial, requires you to take a few steps to make sure your plans include authorization and security. DAC's Anti-Terrorism and Force Protection supports a DOD regulation requiring all employees to complete the Level I Anti-Terrorism Awareness Training, as well as the Defensive Travel Training, within 90 days of traveling overseas — officially or unofficially. DAC also provides a travel briefing and debriefing if your travel takes you to certain countries, and this training is also available to family members. In Defensive Travel Training, DAC helps prepare you for possible incidents so you know how to deal with the threat of terrorism, espionage and other crimes while traveling.

On an average day in DAC, what would we find you doing?

You have to have permission and more importantly a "need to know" or a need to access a special access program (SAP). It is not up to you, it is up to the management of that particular program. Most of my day is helping staff process program access requests, arranging for adjudications for access to SAPs, answering questions and, in general, supporting all the needs for the SAPs that DIA administers.

How long have you been with DAC, and what made you want to work here?

I've been with DAC for approximately five years, and have been working with SAPs since 1997. I was supporting SAPs for the Navy and coming to DIA was a promotion, a nice place to work, a 15-minute commute, and a great opportunity to broaden my horizons and knowledge of SAPs in the intelligence community.

How does your role in security help DIA accomplish its mission?

Sometimes the DIA mission requires extra security. I help secure SAPs so our analysts, financial advisers, engineers and military members around the world can safely and securely complete their mission.



Trina Randall
Security Specialist
DAC-2A1

For unofficial travel, you also need to complete a request located on JWICS at http://www.dia.ic.gov/homepage/da_restored/da/dacsa/systemlink.htm. Please feel free to e-mail questions on JWICS to "Antiterrorism/Force Protection Service" (dise703-dia@DODiis.ic.gov), or call Michael White at (703) 907-2793, Aiyana Oates at (703) 907-1547 or Edward Baker at (703) 907-0934.

Concerns about foreign travel and contacts, suspicious activity, security incidents, and anomalies? Call DAC at (703) 907-1307 so our professional investigators can look into the issue.

DACSecurityAwareness@DODiis.ic.gov

DACSecurityAwareness@dia.smil.mil

DACSecurityAwareness@dia.mil

DAC Supports Deployment

As your intelligence career develops, you can gain special understanding of the agency's mission by deploying. It amazed me during my deployment that all the normal services and support for our troops are in-country, including DAC. In 2004 I deployed to Iraq

to support the Iraqi Survey Group (ISG) and was surprised to find a DAC team already there! DAC had a full-time person assigned

to the ISG for everything from base security to personnel security. There was also a DAC team to train then-MG Keith Dayton's personal security detail, and some of the collectors in the Green Zone too.

A couple years later, I deployed to Afghanistan. I attended a one-week, 40-hour pre-deployment training course, called the DIA Deployment Qualification Course (DDQC), that helped me understand the deployment environment and the skills I needed to stay safe. DAC was there too, providing the Small Arms Qualification Course in case I needed to use a firearm. Having never served in the military, I was glad this training gave me an opportunity to learn about firing a weapon and how to develop my skills over time. DAC also provided Individual Protective Measures Training (IPMT). DAC has researched and designed

an extensive, multi-disciplinary program specifically for DIA personnel in forward operating environments.

Cargo Container = SCIF?

During deployment in a fusion cell, DAC's expertise ensured safe operation of a SCIF in a hostile environment with third country foreign intelligence security services. I was familiar with a SCIF in the DIAC, but a SCIF in the field can be almost anything. I never thought a tent or a cargo container could be a SCIF, but there our SCIF was a trailer inside a building.



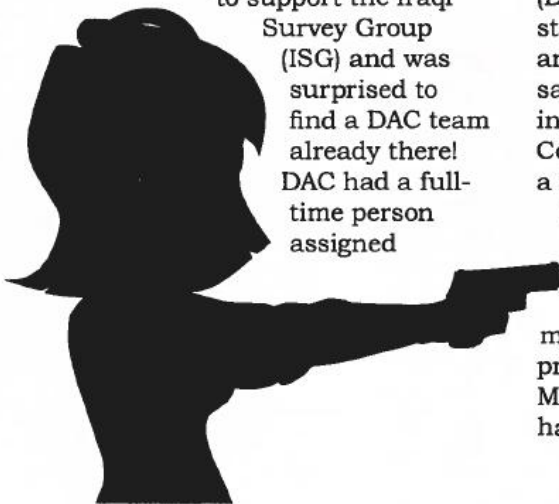
Photo by Michael C. Marynowski, DA



Photo by Michael C. Marynowski, DA

▲ Observers watch tactical assault training in country.

◀ DIA firearms practice in country.



With the exception of the National Reconnaissance Office, National Geospatial-Intelligence Agency and the National Security Agency, DAC grants and maintains the accreditation of all DOD SCIFs. DAC also performs in-country residential security for door locks, and emergency action and destruction plans for diplomatic missions, attachés and DIA staff working at embassies around the world.

The procedures for SCIF accreditation cover conception to construction and continue through its life cycle. A comprehensive risk management approach is used by DAC throughout the accreditation process, which reviews several key factors including:

- Physical security standards
- Protection against surreptitious entry, regardless of SCIF location
- Deterrence of technical surveillance activities taking place within the SCIF
- Tempest security measures for electronic processing of SCI

Tempest is the investigation and control of compromising emanations from telecommunications and computer systems that, if intercepted and analyzed, disclose the information that was transmitted, received or otherwise processed. A compromising emanation could carry data, such

as an image displayed on a computer screen or a page produced by a printer. DIA employees and contractors play an active role in protecting our sensitive information from being lost in a Tempest attack by contacting DAC when

◀ DIA Police Officer Bernard Bryant stops traffic and waves a vehicle into the Clarendon parking facility.

Lt. Darryl Robinson carefully watches the monitor as a scanner reveals what's inside DIA personnel's bags. ▼



Photo by Margan C. Kerwin, CP



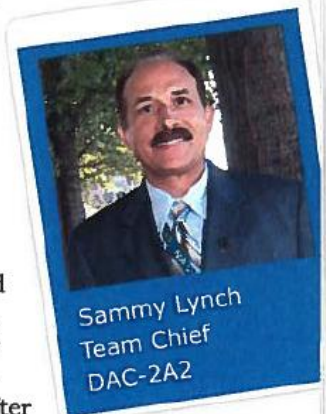
Photo by Margan C. Kerwin, CP

On an average day in DAC, what would we find you doing?

A large portion of my day involves answering requests and questions from DAC customers worldwide. I also interact with other security professionals in the IC to coordinate security matters of mutual interest.

How long have you been with DAC, and what made you want to work here?

While in the Navy during my tour at JAC Molesworth in England, I received great support from some very good people in DAC, so DIA was my first choice for employment after I retired.



Sammy Lynch
Team Chief
DAC-2A2

How does your role in security help DIA accomplish its mission?

My team and I are responsible for approximately three-fourths of the U.S., including Alaska and Hawaii, and overseas locations such as the Philippines, Japan and Singapore. We support more than 1,200 customers with Tempest requirements and SCIF accreditations, construction guidance, decertification, inspection, and staff assistance visits to identify security vulnerabilities. Our first priority is supporting the warfighter in whatever capacity we can to help them accomplish their vital mission. My team's primary role is to administer DOD security policies and programs to protect intelligence, which includes identifying and correcting security weaknesses, inefficiencies, redundancies and/or deficiencies that may place SCI at potential risk.

equipment in a SCIF is being changed or modified. For more information on DIA's Tempest program, contact the SCIF branch at (703) 907-1299.

Safety in the Field

I am a big dog lover, so when I was in the field, I enjoyed watching DAC dogs check vehicles at entry points. DAC experts also taught me how to check my own vehicle before starting it to be sure I was safe. DAC looked over the fleet of government vehicles and ensured each vehicle had the required equipment, and they showed me how to recognize attack scenarios as I moved about the city. We discussed routes to and from the embassy, choke points and safe havens in the event of an attack, reinforcing my earlier IPMT experiences.

DAC helped me gain a better appreciation for the in-depth security measures I



Photo by Russell D. Roberts, DA

TSCM's Andrew Vavra listens for devices in everyday objects, such as walls, floors or furniture.

immediately to reports of serious incidents involving DIA personnel and family members, workplaces, residences and vehicles. A few months ago while in the field, a DIA employee suspected he might be under surveillance and reported it to his local security officer, who informed

the defense attaché, who in turn reported it to DAC. DAC helped refresh the individual's vigilance and surveillance detection, and provided him with actions he could use to reduce his risk. In situations like this, DAC can enlist support from the State Department to resolve or mitigate threats.

On another occasion, a defense attaché relayed an incident about a colleague in a high-crime and high-terrorism post who was receiving death threats on her cell phone. She sent a Modest Warrior report and received immediate guidance from DAC to implement temporary adjustments to her schedule and activities, and surge protective measures by the regional security officer. DAC coordinated with the State Department, and investigations by the security officer with the local police assessed the probable source of the death threats. DAC enacted all existing protective measures until permanent security measures reduced the risk.

Anti-Terrorism and Force Protection

Anti-Terrorism and Force Protection provides different kinds of security to DIA and selected DOD organizations to protect

passed through from the moment I entered the main gate of the embassy to the time I reached my office. DAC also answered all questions and concerns, from the ambassador to the regional security officer to our locally hired drivers — the DAC representative was a full-spectrum security expert. They ensured compliance with applicable security standards, and became an advocate to make certain we had the right protective measures.

Modest Warrior is a program that allows DAC to respond

While traveling overseas, I recommend you keep a low profile, be alert, be careful and protect critical information. Here are a few tips to keep in mind:

- If you plan to drive while overseas, you may need an international driver's license. Check with your insurance company to make sure you have international coverage.
- When you arrive, ask for a room between the second and seventh floor. This makes it harder for an adversary to reach you.
- Report questionable relationships and foreign contacts to DAC right away.

Anti-Terrorism and Force Protection Team
Phone: (703) 907-1899
Fax: (703) 907-0677
E-mail: dise703-dia@dodiis.ic.gov



personnel, operations, activities, information and facilities from foreign intelligence, terrorism and criminal threats worldwide. This is accomplished in three branches: Field Support, Operations Support and Technical Services.

The Field Support branch is the DOD executive agent for

diplomatic security matters, and security assessments, advice and assistance to approximately 238 defense attaché offices and forward operating bases around the world.

The Operations Support branch runs three programs, including Anti-Terrorism and Force

Countermeasures (TSCM) is where the experts who find electronic listening devices in almost anything reside. And they respond wherever they are needed. My office in an embassy had a conference room located next to an office where foreign national employees worked. We soon realized they could overhear conversations in our conference room. A TSCM expert came to conduct a survey, commonly known as bug sweeps, and it did not take long to find the problem. He determined the wall that separated the two rooms had been soundproofed, but recent air conditioning renovations had not been treated for acoustical security. An air duct penetrating the wall was not wrapped or lined with sound-absorbing material specified in the renovation plan. The problem was quickly fixed.

Employee Career Security

Counterintelligence seeks to stop adversaries who want to know what you know or what you have access to, and they will use any means they can to get you to share that information — this is why counterintelligence is so important.

DAC Counterintelligence and Security focuses on DIA people, property and information to



Photo by Margan C. Kerwin, CP



Photo by Margan C. Kerwin, CP

K-9s and their handlers provide a critical level of protection to DIA facilities. While performing a vehicle check, Jett, a three-and-a-half-year-old black Labrador, indicates he's found something suspicious.

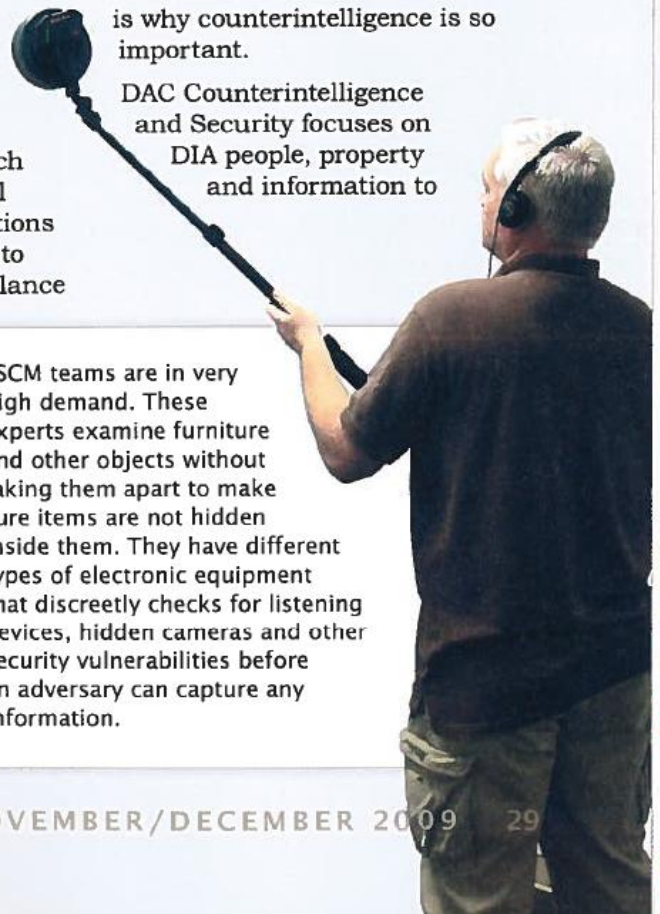
Protection, Protection Assessment and Assistance Visits, and serves as the lead security officer for DIA's Clarendon facility.

The Technical Services Branch carries out complex technical counterintelligence investigations using specialized equipment to eliminate clandestine surveillance devices, or "bugs," in secured facilities.

DAC and TSCM

When you think of all the electronic listening devices you see in the movies, it makes you wonder whether we do that kind of thing in DIA. Well, DAC's Technical Surveillance

TSCM teams are in very high demand. These experts examine furniture and other objects without taking them apart to make sure items are not hidden inside them. They have different types of electronic equipment that discreetly checks for listening devices, hidden cameras and other security vulnerabilities before an adversary can capture any information.





identify and address internal threats. This differs from what most people think of as counterintelligence which traditionally has an external focus. External counterintelligence is performed in the Office of Analytical Support in the Directorate for Counterintelligence (DCA/DC).

DAC Counterintelligence and Security helps employees

understand three things. First, as a DIA employee, you are a target and responsible for security. Second, it is important to be able to identify a threat and know what to do when you see one. Third, you need to know DAC is here to help you, so call us whenever you think something is amiss, even when in doubt, at (703) 907-1307. The main threats to DIA include foreign intelligence services, technology exploitation, unauthorized disclosure and unauthorized release.

Throughout everyone's career, there are life events and situations that could impact security, such as financial issues or pressure from working in the intelligence

field. There are resources available in DIA that can help save your or a colleague's career before a problem develops into something serious.

As we move through our career in the IC, we are all part of the counterintelligence effort to watch and report security concerns to DAC. It is easy to remember cases like Ana Montes, but the most important part of Montes and cases like hers, is the number of years she and others spent operating on the inside. Counterintelligence and Security is here to look at many seemingly unrelated bits of data or information to detect patterns that indicate an internal threat.

Although DAC's counterintelligence mission looks inward for possible signs of espionage or other security problems, we all have a responsibility to be vigilant

The Best of the BEST PRACTICE for the WORST

By Alexander F. Wojcicki, DA

Have you ever wondered what would happen if something hazardous to the work force came through the mail? If you were at the DIAC Sept. 24, you would have been able to find out firsthand. Exercise East Wind 09 was a full-scale exercise designed to assess DIA's capability to respond to a weapons of mass destruction incident at the DIAC's Remote Delivery Facility (RDF).

When the alarm rang in the RDF, Directorate for Mission Services Office for DIA Information and Special Services (DA/DAN) mail handling personnel immediately activated their emergency response procedures, locking down the building and evacuating. DIA Police quickly secured the site, and tested the air around the facility with special sensors to determine the presence of hazardous materials.

For approximately three hours, real-time notifications and response protocols were conducted. First responders from Bolling Air Force Base and Naval District Washington (NDW) were on the scene in



Naval District Fire Department Capt. Kevin Grinder manages the emergency response activities during an exercise involving the Remote Delivery Facility at the DIAC.

and report any suspicious activity — even if it's a co-worker or friend.

DAC has certified officers who are responsible for counterintelligence and security investigations. They officially represent DOD and DIA, and have been specially trained and authorized to conduct investigations, carry firearms, perform counterintelligence duties and conduct personnel security investigations — some are even certified by the U.S. Marshals Service to make arrests.

Security Within Industry

DIA depends on industry and the expertise of contractors for help to complete specific and timely work. DIA supports a “one team, one mission” work environment, and although there are some differences between what government employees and

contractors can do, we all protect classified information.

DAC conducts security checks for each of DIA's industry partners. There are more than 12,000 cleared contractor facilities in the U.S. that contribute valuable services to DIA, as well as to executive branch agencies. The National Industrial Security Program is administered by DOD's Defense Security Service. It levies very stringent requirements on industry for the protection of national security information.

DAC's Industrial Security team ensures that security procedures and safeguards are effectively integrated into the life cycle of all

contractor bids, proposals and final award efforts. Through a careful review of security documentation required by the Federal Acquisition Regulation, the DAC Industrial Security team works with the Office of the Acquisition Executive (AE) and subject matter experts to ensure contractors are aware of critical security requirements, access restrictions and other mandated requirements for handling classified information. Realizing that most DIA contracting officers and their representatives are not security professionals, the Industrial Security team reaches out to educate contractors on security matters and to help with contract classification specifications, statements of work, classification guides and contract-specific security addendums added to a DIA bid.

minutes. A unified incident command composed of DIA Police and NDW Fire was established and controlled the actions of all responders on the scene.

“This was a great opportunity to bring together DIA with agencies from our host installation,” said Michelle Buteau, exercise director and deputy chief of the Office of Enterprise Operations Mission Assurance Division and Situation Center (DAE-1). “We appreciate the opportunity to train with our response partners and plan to take what we learned and continue to enhance work force protection.”

DIA participating agencies included DAE-1, the Counterintelligence and Security Office's (DAC's) Anti-Terrorism/Force Protection Office and DIA Police, and DAN's Courier and Mail Services. DIA's exercise planners worked with personnel from the Center for National Response, a part of the West Virginia National Guard Joint Interagency Training and Education Center. More than 50 responders participated in the exercise. ☐



During the exercise, DIA Police Officer Dustin Smith gets scrubbed down outside of the Remote Delivery Facility at the DIAC.



Photos by Margan C. Kerwin, CP

“Proactively looking at ways to safeguard valuable information is critical to DIA’s success.”

Solid Security in a Digital World

Over the past 20 years, the importance of technology at DIA has skyrocketed. On one hand, all the advances in technology provide instant communication and a world full of information and knowledge. However, each new technology brings with it new security risks. DAC recently stood up a capability to address technological risks, the DAC Cyber Division. This division has three main focus areas: cyber investigations, insider threats and operational security (OPSEC) operations.

The Cyber Investigations team provides computer counterintelligence and criminal investigative expertise and support for all investigations and suspicious activity involving computers. DAC special agents trained in cyber investigations assist other investigative agents, both within and outside DIA, with computer forensic analysis and interviews of individuals where technical terminology is used, just to name a few. DAC special agents focusing on cyber counterintelligence formulate relationships within the cyber community and stay abreast of current and emerging threats. They give crucial insight into attack vectors targeting DIA and the ever-changing threat landscape.

The Insider Threat Program is a robust, all-source threat analysis and anomaly detection program. The system leverages information resources in DIA and across the government to provide

a big picture of activities and events using complex algorithms to highlight areas of interest in data streams that are far too large to view manually. This capability spans both physical and cyber domains, and can provide all-source support to damage assessments following the detection of an event.

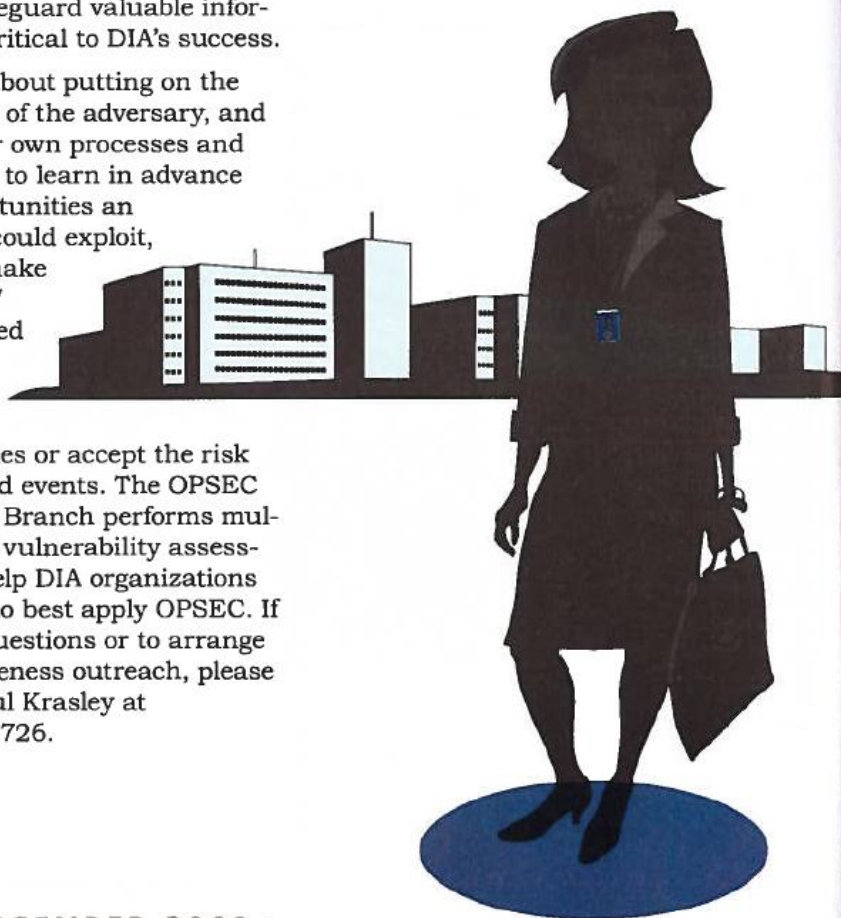
OPSEC is the protection of unclassified but sensitive information, and the OPSEC Ops experts from the DAC Cyber Division help protect this valuable data from adversaries. For example, Sept. 11 and the USS Cole and Oklahoma City bombings were planned and executed with unclassified information. Proactively looking at ways to safeguard valuable information is critical to DIA’s success.

OPSEC is about putting on the perspective of the adversary, and casing your own processes and procedures to learn in advance what opportunities an adversary could exploit, and then make smart cost/benefit-based changes to eliminate those opportunities or accept the risk of undesired events. The OPSEC Operations Branch performs multidiscipline vulnerability assessments to help DIA organizations learn how to best apply OPSEC. If you have questions or to arrange cyber awareness outreach, please contact Paul Krasley at (703) 907-2726.

Retirement and DAC

I started this journey looking back at my career as a DIA analyst who over the years learned about my responsibility to protect DIA’s people, property and information. I hope some of the points I’ve shared with you will help you during your career. Leaving DIA is not the end of my responsibility to preserve security. As I retire, DAC reminded me of my oath many years ago to protect national security — and it will continue.

The intelligence community, DOD and the federal government are looking for ways to collaborate, communicate and integrate missions with shared resources. Social networking and technology will continue to provide DIA with new tools to collect, analyze and share information. And DIA will be looking to DAC and the security experts in DIA to find ways to use technology in a security environment. ☛



KISS My PowerPoint — Keep It SIMPLE

By Brian D. Nickey, CP

From font to color to animation, these tips guide you in what to do — or not to do — to improve the look and effectiveness of your presentations.

Whether you're briefing your boss, giving a presentation to a class or making a slide show to highlight a family vacation, the design principles you use remain the same.

You don't need to be a graphic designer to put together attractive presentations, but knowing a few simple tips can make them look better, and, more importantly, keep your audience's attention.

Before we get started, if you're giving an official DIA brief, make sure you use the new standard DIA template and follow the guidelines accordingly. You can find the template on both JWICS and SIPRNet on the Internal Communications home page and in the DIA Correspondence Guide.

Sometimes people tend to think more is better, but in design, less usually provides a more pleasing composition. I've always liked the Army approach of "KISS" — keep it simple soldier. KISS makes a lot of sense in graphic design. Your presentation design and graphic elements should enhance and reinforce your message, not distract or confuse your audience. Having too many fonts, going crazy with colors, or haphazardly using software graphic elements and features can ruin a briefing. The following few tips can lead you down the road to better looking presentations.

Design 101

FONTS, fonts & more fonts

Today computers come loaded with tons of great fonts and endless possibilities for fun projects. Legibility is the number one priority when selecting a font. If your audience can't read it, what's the point? This means looking at both the size and style of the font, as well as how much information is on your slide. Less is definitely better and more effective.

In addition, use an appropriate font for your message. My 11-year-old daughter

recently had me proof a science report that was typed entirely in her new favorite font, "Curlz." Needless to say, we had a little more work to do before turning it in to her teacher. If you want your audience to take you seriously, make sure your font choice reinforces that message.

Also, don't use too many fonts. It's easy to get carried away and use lots of these cool fonts to spruce up your presentation. Try to avoid these temptations by sticking to

only two or three fonts. If you feel you need more, use different variations of a single font, such as light, bold, condensed or italic to create contrast or draw attention. But keep in mind that many attractive designs only use one font.

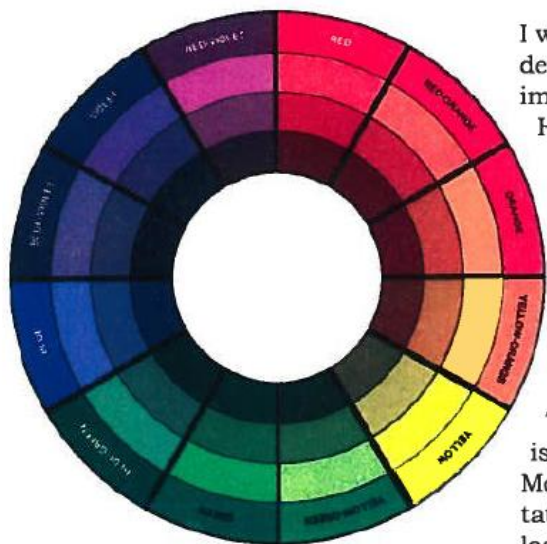
OK, now that we're learning to control our font urges, let's move on to color.

Color Me Bad

Color is another area where it's easy to get carried away. Many people don't give much thought to color as they're putting together their presentations, but color is a great mood setter, and most colors carry physiological, cultural, personal and emotional implications. Colors like red and orange suggest warmth and seem to move toward the viewer, thus appearing closer and larger. Cool colors like blue and green suggest coolness and seem to recede and appear smaller. You can get away with using larger areas of cool colors without overwhelming the viewer.

As with fonts, don't use too many different colors. Try using a monochromatic or analogous color scheme. Monochromatic color schemes only use a single color but have different shades or values of that color. Analogous color schemes contain a common hue





and are found next to each other in the color wheel, for example red-orange and red-violet.

Also, use a color scheme that relates to the subject. Once on a home design show, the designer made a good point when she said, "Just because it's your favorite color, doesn't mean you should paint an entire room with it." If

I were creating a series of slides demonstrating the effects of an improvised explosive device on a Humvee, I wouldn't use bright yellow, pink and purple just because I liked those colors. I know it sounds like common sense, but you'd be surprised.

Just because you do something, doesn't mean you

The last exercise in restraint is that of playing with new toys. Most people develop their presentations in PowerPoint, which is loaded with great features. The key is to resist the temptation to use some of these features that don't add value to message. One example is the WordArt tool. WordArt allows you to apply any number of graphic techniques to your words, such as curves, shadows and slants. If you must use it, only apply one style to your slide and keep it simple.

I'm a big "Star Wars" fan, but I can't tell you how many times I struggled through briefings that had every transition technique available — you know those individual letters flying in from all directions complete with sound effects! These animations, while amusing, can really weigh on your audience and even irritate them. I prefer to not use any transitions at all, but if you do, limit it to just one simple technique.

Not everyone is a designer or creative by nature, but if you follow these few tips, you can improve the look of your briefings, and more importantly, not distract your audience. Bottom line, ensure all the elements you choose reinforce your message, and if anything detracts or distracts from your message ... get rid of it. Remember, sometimes simple is a good thing. ☺

COMMUNITY OUTREACH

EUCOM JAC Enlisted Leader Meets WWII COUNTERPART

By Peter G. Park, EUCOM

A modern-day sailor meets with a World War II veteran to talk about Hell's Angels and a new award for today's enlisted service members at JAC Molesworth.

MCPO John Frakes and U.S. Army Air Corps Master Sgt. Fabian Folmer both served their country in Molesworth, England. They were just 66 years apart.

Despite the passage of time, the roles of the two men are similar. Frakes leads today's enlisted corps supporting the analytic mission at the EUCOM JIOCEUR Analytic Center (JAC). Folmer led the mechanics of the 303rd Bomb Group (Heavy) who kept the famous B-17 Flying Fortress Hell's



1944: Master Sgt. Fabian Fulmer and the crew of Hell's Angels visited the set of "To Have and Have Not." Folmer is front row, between Humphrey Bogart and Lauren Bacall.

Photo courtesy of 303rd Bomb Group Association

Angels operating out of Molesworth against Nazi Germany from 1942 to 1944.

Their two paths crossed in August when Frakes traveled to the Midwest to meet Folmer.

So why was today's JAC senior enlisted leader in Osage, Iowa, visiting the now 91-year-old retired Folmer?

Well, JAC Commander Col Pete Devlin created a new JAC award for enlisted members in support services who make the analytical mission possible. With existing JAC awards named for intelligence officers with the wartime 303rd Bomb Group, it was natural to find a 303rd member who epitomized excellence in support services to name this new award after. Hell's Angels crew chief Folmer was the obvious choice.

Hell's Angels was the first B-17 to complete 25 missions, finishing its 25th several days before the more famous Memphis Belle. While the Memphis Belle was sent back to the U.S. on a war bond tour, Hell's Angels soldiered on, surviving 48 missions before it, too, went back to the United States. Folmer was there, touring war plants and Hollywood, where the crew visited the set of the Humphrey Bogart movie "To Have and Have Not."

Folmer played such a critical role in the operation of Hell's Angels, an entire chapter entitled "Fabulous Fabian" is devoted to him and his crew in the book "First of the Many: Journal of Action with the Men of the Eighth Air Force" by John R. McCrary and David Edward Scherman:

"Fabian Folmer, from Mansfield, Ohio, twenty-five years old, married, father of a six-months-old baby girl born after he left the States, is the crew chief of a very big baby, the famous Fortress Hell's Angels. ... There is a strange and strong relationship between a pilot and his crew chief — stronger than between any other two men in the air corps, stronger often than the tie between pilots and co-pilots."



Photo courtesy of artist Keith Hill

JAC Senior Enlisted Leader MCPO John Frakes meets with former U.S. Army Air Corps Master Sgt. Fabian Folmer, crew chief of the famed B-17 Flying Fortress Hell's Angels. Folmer signed copies of the painting "Molesworth Dawn," pictured left, which will be presented to award winners. Folmer is pictured at left as the crew chief under the propeller hub.



Photo courtesy of Mitchell County Press News

"When I tell a pilot that my plane is 'ready for combat' he's got to take my word for it," Folmer said at the time. "Sometimes, you sort of flinch when you say it, especially in the beginning, because you know so much depends on your being right. I haven't been wrong yet."

When Frakes traveled to the JAC Minneapolis reserve site recently, he drove to Osage and met with Folmer. Folmer signed prints of the painting "Molesworth Dawn," in which he is depicted. These prints will be presented to recipients of the Master Sergeant Fabian S. Folmer Award for Excellence in Support Services, the first of which will be in the spring of 2010. 🌟

The *Communiqué* staff interviewed one of the agency's departing "legacies" and asked her to share her career experiences and a few words of wisdom.

If you wish to nominate an individual who is retiring, please contact Margan Kerwin at (703) 697-8781.

Sandra Gemmell

How long have you been with DIA, and where have you worked within the agency?

I was first employed in 1981 by the U.S. Embassy to work in the DIA Liaison London (DIALL) office as an intelligence information clerk. At that time there was another U.K. national, Margaret Jordan, working for DIALL in the capacity of personal/administrative assistant. In 1990, she retired after service spanning 27 years, and I was promoted into that role.

What are your fondest memories with the agency?

My fondest memories are associated with the numerous chiefs and liaison/exchange/integrated officers who have been assigned to DIALL over the years. Each one had a unique personality and brought something different to the office, with some finding it easier than others to integrate into the British working and social arenas. Sometimes we really don't speak the same language, and some interpretation is necessary. I have enjoyed watching how people react to working so closely with the Defence Intelligence Staff (DIS) and other U.K. agencies during their tour in London. Most will return to DIA headquarters with a broader understanding of the strengths and limitations of the much smaller intelligence community in U.K.

What lessons did you learn throughout your career that you would pass on to others?

Try to treat everyone you meet or talk to, for whatever reason, with equal courtesy and respect.

Do not be afraid to voice an opinion. Sometimes it's easy to sit back, say nothing, then say "I knew that would happen" rather than enter into what could be a difficult discussion at the beginning. Don't assume those in a position to make decisions have all the information you have. Also, it's no good just saying "no, you can't do that" to someone — be prepared to back it up and come up with an alternative solution.

Another big lesson I learned over the years is that an action request passed to me personally is an action request I was duty-bound to follow until the response was finalized. Passing it on to someone else and assuming they will respond to the originator is not an action closed.

What would you consider to be your greatest contribution to DIA?

Loyalty — to the agency as a whole and to DIALL. There is a great working relationship between DIA and DIS, but I don't think anyone will disagree that sometimes there is "agreement to differ" over some issues. I have



Photo by SrA Jaclyn McDonald

tried not to let personal opinion as a U.K. national interfere in my work. That's not to say I'm backwards at voicing my opinion — as I'm sure many will agree.

What do you think has been the biggest change or had the biggest impact on DIA during your career?

Technological advances, without a doubt. When I joined DIALL it was still a novelty to have IBM Selectric II correctable typewriters and a KY3 phone! Our first computers were three stand-alone WANG systems. We had limited connectivity with U.S. Naval Forces — Europe (USNAVEUR) in the early 90s, but really didn't get connected to DIA headquarters and the wider world until the mid-90s. I think this connectivity and the huge amount of information available online has, to a large extent, driven how we work.

Do we control the information or does the information control us? Sometimes I'm not sure of the answer.

On a simpler note, how many people actually have face-to-face contact with people they "work" with every day? The tendency to sit in the office and e-mail (far too many of them!) rather than make the time to go and talk to someone sometimes distorts our perceptions of people and situations. Visual and personal communication skills, and also some problem

solving skills, are being lost. The decision to put administrative information, which I used to see as a matter of course in hard copy, on a national high-side system has made it harder for me as a foreign national to have all the information I need to do my job as well as I would like.

Do you have any final words of wisdom you would like to share before you part from DIA?

It's sometimes easier to follow the crowd, but if you have an opinion

on a situation or you have a sound reason for disagreeing with a set of facts, figures or proposed plan of action, then say so. I don't think the agency or its seniors are served well if we are not prepared to challenge ideas or ways of doing things.

By the same token, don't be afraid to change your opinion. It just means you have taken a balanced view of information now available to you and recognized that a previous belief was perhaps flawed — it is not a sign of weakness. ☛

PEOPLE ON THE MOVE :

Civilian and Military PERSONNEL UPDATE

Retirements, Anniversaries and Promotions in June, July and August 2009

By the Office of Human Resources, HC

Civilian Retirements

Robin B. Boatman, DI
Thomas R. Carroll, SOCOM
Daniel M. Crosby, HC
Clemons Cumbee Jr., STRATCOM
Joseph A. Cummins, DI
Deborah I. Curtis, EUCOM
Edward C. Ferriter, CP
Thomas F. Haigler, USFK
Judy D. Harne, DI
David Harper, IG
Randy L. Huffer, DI
John L. Kmetz, DI
Theodore M. Laven, CE
Eric Mastroianni, DH
Ronald I. Miller, DI
Takeo Nemoto, DH
Elizabeth C. Pickering, MC
Daphne E. Poblete, IE
Harold R. Shapiro, DH
Douglas L. Smith, EUCOM
Marilyn B. Sorrell, EO
Richard E. Tisdell, DI
Herman V. Triplett, DH

Employee Celebrating 45 Years Federal Service

Toussaint C. Griffin, DS

Employees Celebrating 40 Years Federal Service

Patricia R. Shepherd, DI
Lily G. Tobani, DH
Brenda K. Zeliber-Richards, DA

Employees Celebrating 35 Years Federal Service

Florence Abney, HC
John J. Aclin Jr., CE
Thomas N. Baker Jr., J2
Dorothy H. Blackwell, MC
Howard B. Buchanan, HC
Norman R. Denny, DI
Michael R. Freed, IE
Karrie S. Friedlander, IE
Joseph S. Gordon, MC
Carol A. Hilliard, DS
Donna M. Hubbard, TRANSCOM
Stephen E. Kinker, USFK
Lori A. Kreger, DJ
Frances K. Lucas, DI
Dolores L. Wyatt, JFCOM
Christopher B. Yates, DT

Employees Celebrating 30 Years Federal Service

Warren G. Anthony, IG

Guy R. Arrigoni, DI
Kara A. Byrd, DS
Salvatore L. Calfa, DS
Carol L. Campbell, DS
Beth A. Cary, DC
Anthony E. Cerullo, DI
Aaron N. Cooper, FE
Michael D. Coulson, TRANSCOM
Leo J. Delaney, DI
John J. Devine, HC
Harry A. Frank, J2
Wyndolyn D. Fuqua, DI
Cynthia K. Geis, DI
Brenda W. Glasbrenner, J2
Dorgia A. Kent, DA
Paul D. Lane, DA
Ava M. Martin, DS
Daniel S. Mauck, DT
Laurie A. McMahan, DS
Richard E. McQuiston Jr., MC
Lisa L. Morgan, DX
Paul A. Murad, DI
Esteban Rodriguez, DH
Marshall G. Smith, DH
Dennis W. Sumner, DI
Barbara J. Werre, DI
Kathy L. Williams, DI

**Employees Celebrating 25 Years
Federal Service**

Darryl M. Bennette, DI
Lida M. Christian, DI
Lucille B. Cuffy, HC
Sherma K. Donovan-Beckford, DC
Mark R. Fahner, MM
Philip B. Ferguson, DC
Ilsa E. Ferro, DA
Evelyn A. Francisco, DA
Van W. Garraghty, AFRICOM
Jacqueline D. Graham, DA
Leslie S. Gulyas, DT
Michael A. Halladay, DT
William E. Hiestand, DI
Carshena Y. Holladay, JFCOM
Edward W. Hopkins Jr., DI
Kelly R. Hughes, DX
Finis B. Jeffery, DI
David M. Kashmere, DI
Duff G. Kelly, EUCOM
Catherine E. Landon, DH
Veltina S. Lane, DA
Gary F. Markham, AE
Norman A. Mash, PACOM
Bobby C. Mask, SOUTHCOM
Delores L. Matthews, AE
Sonya R. Medlock, DI
Tammy D. Mitchell, HC
Marc A. Mullin, DH
Brenda G. Ozi, DS
Court A. Rawson, EUCOM
Sharon A. Shelton, DS
Dan L. Strode, DI
Duane Tatchyn, DH
James A. Vardy, DA
Michael P. Vaske, DT
Paul H. Vivian, DI
Benjamin D. Watkins, DA
Michelle A. West, DJ
Sharon D. Wiley, DA
Debra E. Williams, DI
Wanda J. Williams, DI
Sandra L. Woodard, DX

**Employees Celebrating 20 Years
Federal Service**

Ann H. Adams, DI
William J. Bagley, DI
Matthew A. Boczek, DI
Amy L. Boward, FE
James T. Brady, DI
Thomas P. Brown, DC
Kenneth R. Brunjes, EUCOM
Jeffrey P. Burke, DI
Mark C. Butler, DI
Janene E. Chase, DI
Michelle F. Cook, DI
Keith A. Crompton, STRATCOM

Joan A. Dickerson, CENTCOM
Martin D. Dunn, JFCOM
Denise Facey, HC
Edwin J. Faller Jr., TRANSCOM
Patsy L. Fifer, DH
Michael T. Gilpin, DC
Larry J. Graham, SOCOM
Maurice H. Guffey, STRATCOM
Randy L. Hack, DI
Mark K. Harrison, CP
Richard L. Hartnett, DI
Michelle L. Henderson, DI
Shane W. Higgs, DX
Mark F. Hines, DI
Erika R. Holmes, DI
Alita D. Hunter, DS
Lorie K. Hutton, DC
Ann K. Inouye, PACOM
Jeannie L. Kinzler, DH
Paul L. Lago, DI
Martin H. Lindsey, DI
Cynthia D. L. Little, DS
Kevin E. Locke, DA
April L. Maletz, JFCOM
Arleen B. McCauley, PACOM
Thomas M. McCullough, PACOM
Shelby K. McDaniel, HC
Angela R. Middleton, DS
David M. Moretti, JFCOM
Kenneth W. Murphy, FE
Michael C. Needham, STRATCOM
Caleb G. Neirman, DH
Gregory F. Nero, DI
David J. Ohara, DJ
David V. Owen, DC
Marcia D. Parker, DI
John V. Perroots, DH
Yulondia C. Pettigrew, DS
Karen N. Poole, FE
Melvina M. Rice, HC
Jesus J. Rodriguez, DH
Brenda D. Smith, DI
Jennifer L. Snellings, DA
Susan Sternad-Basel, DS
William J. Tehan, HC
Margaret T. Watson, DI
Amy L. Weed, DI
Yonnette G. Weithers, DI
Donna M. Welch, DA
Edward H. Westfall Jr., SOCOM
Cathy E. Whitehead, DI

**Employees Celebrating 15 Years
Federal Service**

Mark C. Andreadis, DH
Felicitia L. Barranco, DI
Barry R. Billmann Jr., DI
Preston K. Birchett, DH
Marianne B. Carlson, DI

Nicole K. Chaney, EUCOM
Jan C. Chrypinski, DI
Laurissa O. Corrales, CENTCOM
Chester D'Ascendis, EUCOM
Michael S. Donovan, DI
Matthew S. Eggleton, AFRICOM
Gloria S. Evans, HC
John Frendak, DA
Leroy M. Garza Sr., DA
James P. Gerhard, DI
Jason S. Gilman, DA
Suzanne M. Heigh, DT
Zachary D. Herzer, DH
Arturo M. Holston, DH
Bobby R. Horne Sr., DA
Anthony J. Hunter, DI
Manuel E. Joza, PACOM
Doris E. Kirsch, EUCOM
James M. Krushat, DI
Lydia Lopez-Bolden, DI
Eric Maddox, DH
John L. Miller, DA
Joy M. Miller, MA
Deborah Monroe, DI
Kathryn L. Morici, DI
Valarie C. Noel, HC
Gustav A. Otto, DC
Katrina A. Reisinger, IG
Joseph O. Sams, DI
Thomas C. Smith, DJ
Terry M. Stahl, MC
Todd L. Strawser, CE
Mark B. Taylor, DT
Charles H. Tudor II, DH
Wayne Washington, FE
David W. Weed, DJ
Joseph R. Whitaker, DI
Rachel M. Wilson, DC
David H. Yuninger, DX

**Employees Celebrating 10 Years
Federal Service**

Fredesvinda Adams, DA
Robert E. Allen, J2
Michael J. Anderson, DS
Luis A. Ayala, DA
Scott C. Baker, DA
Gabriel F. Barreiro, EUCOM
Gregory A. Brewer, CENTCOM
Marcus J. Brown, AFRICOM
Kris R. Campbell, TRANSCOM
Jean-Paul L. Chaine, AFRICOM
Lynne M. Champion, IG
Thomas R. Chesney, DS
Larry N. Cobey, DA
Lawrence J. Cole, PACOM
Clyde C. Crane IV, J2
Carrie L. Crawford, CS
Christopher L. Dryden, DI

Kevin S. Feagin, DJ
 Ronnie Foxe, HC
 Andrew J. Funk, DI
 Michael G. Geiger, DX
 Sandra Gemmell, IE
 Levi H. Gossett, SOCOM
 Thomas H. Grimes, DI
 William J. Groller, DI
 Mia R. Guzman, DI
 Darren R. Guzzone, DA
 Jennifer L. Halston, DJ
 Gerald W. Hamrick, DET420
 Charles C. Hartzog, DC
 Donna J. Hersherberger, DH
 Jon M. Hinchcliffe, CENTCOM
 Nicholas A. Hughes, DI
 David L. Ikeda, PACOM
 Gary E. Isom, DH
 Michael V. Jernigan, EUCOM
 Artesa D. Jones, AFRICOM
 Cherie Jones, DA
 Young S. Kim, DI
 Theresa Renee King, SOCOM
 Max M. Kingsley, DH
 Alexander K. Kuhns, NMEC
 Kenneth A. Leadbeter, DA
 William F. LeFever Jr., DT
 William J. Lifsey, MM
 Heather R. Lownes, IG
 Arnalda N. Magloire, DI
 Kristean E. Marchant, DI
 Jonathan R. Martinez-Aponte, DI
 Stanli O. Montgomery, DI
 Renee L. Morris, DA
 James P. Nock, NORTHCOM
 Judy A. Pike, DH
 Michael A. Plaisted, FE
 Christopher C. Powell, DI
 Colin I. Powell, DX
 Joy D. Procaccio, EUCOM
 Michael Ragin, DH
 Jodi G. Riddell, DI
 Robert G. Rieser, DT
 Mark C. Ritter, DC
 William E. Roach, DI
 Jason W. Roberts, HC
 David J. Romett, EUCOM
 Brian C. Sample, DI
 Veronica N. Shibley, CE
 Teresita G. Smith, DJ
 John W. Snyder, HC
 Larry G. Stotts, DH
 Nicole K. Swartz, DC
 Scott Sweedler, DI
 Peter M. Szekely, EUCOM
 Jasen O. Tanner, DI
 Adam E. Thode, DC
 Jennifer J. Thorpe, DI
 Justin T. Thurber, JFCOM

Christopher J. Ventura, DI
 Damon J. Wilson, DC
 Karludie Young II, DH
 Deborah A. Younge, DI

DIA Promotions to DISL

Wayne K. Davis, DX
 Lisa H. DiGregorio, DH
 Thomas L. Donnelly, DJ
 David P. Ridlon, DX
 Yvette C. Wooley, DJ

DIA Promotions to Pay Band 05

Melinda K. Baran, DI
 Russell A. Battaglia, FE
 Daniel L. Burghart, MC
 Terry S. Carter, FE
 Pedro A. Chevere, HC
 Daniel D. Coates, CENTCOM
 Jordan B. Davis, EUCOM
 Anita M. Groves, SOUTHCOM
 Gary R. Hill, CS
 Edgar Hollandsworth, DJ
 Rick L. Hueston, DI
 Thomas C. Kuhns, DI
 David K. Martineau, DH
 Terry R. McFarland, HC
 Jacob P. Merciez, DI
 Melanie Y. Moore, AE
 Scott R. Patterson, DX
 Charles F. Perkins, DA
 Jennifer H. Sylvestre, AE
 Sandra L. Woodard, DX
 Ryan M. Zimmerman, DX

DIA Promotions to Pay Band 04

Charles T. Aaron Jr., DS
 Guillermo Alcover-Muniz, SOUTHCOM
 Michael N. Alexander, STRATCOM
 Maria A. Baker, DI
 Jason G. Cameron, DA
 Jillian L. Carilli, EO
 David W. Chambliss, CENTCOM
 Peter A. Chevere, DI
 Janie M. Church, DA
 Glenn A. Conklin, DA
 David M. Eltinge, DA
 Warren A. Epes, DA
 Susan E. Fink, DT
 Lawrence J. Finnery, DH
 Andrew C. Franks, DH
 Mitchell K. George, DH
 Stuart M. Gold, AFRICOM
 Young H. Han, HC
 Shelley R. Hardy, EO
 David L. Hawkins, DI
 Andrew L. Headley, DX
 Kenneth R. Hlavaty, CENTCOM

Stephanie R. Hollaway, HC
 Ryan R. Howell, DH
 Holly L. Knorr, DI
 Mark J. Laurent, DI
 Sarah L. Martin, CP
 Leigh C. Matiunas, EUCOM
 Jack D. May, DI
 Katherine M. McCloskey, DI
 Deborah M. Melancon, CE
 Joshua M. Michaud, DI
 Manuel Antonio Montalvo, DX
 Matthew F. Moseley, DI
 Darren S. Mott, DX
 Weston W. Ochse, DX
 Harold Odrick, IG
 Shannon L. Paschel, DI
 Austin L. Pearl, DI
 Jaime E. Ramos, DA
 Anthony D. Scaife, DA
 Lisa J. Schrenk, DS
 Kristin J. Seward, DH
 Travis R. Thompson, EUCOM
 Traber S. Michael, DT
 Erin L. Valocsik, DI
 Robert L. Wilke, DI
 Jessica H. Willis, DA
 Amy K. Wolf, DH
 Marc J. Zuccola, SOCOM

DIA Promotions to Pay Band 03

Patrick J. Adams, FE
 Adam C. Arnett, DI
 Sherita R. Banks, HC
 Filomeno G. Batayola, PACOM
 Elizabeth Marie Cilia, DI
 Lolita O. Clarke, FE
 Joseph A. Cutler, DI
 Joshua A. Danny, DI
 Karen M. Dize-Hart, DA
 Scott M. Dominick, DX
 Maureen A. Eichelberger, MC
 Jessica A. Eidson, DI
 Michael A. Faino, DI
 Iftin A. Fatah, FE
 Leishvanette M. Figueroa-Ramirez, DI
 Carson M. Frederick, DH
 Megan E. Gooch, FE
 John L. Gypson, DI
 Tarah S. Hancock, FE
 Linda M. Harrell, HC
 Donita L. Harris, DH
 Jerome R. Heffner, DI
 Vanessa E. Holder, DI
 Angela Johnson, DA
 Corisha M. Johnson, DC
 Jennifer L. Johnson, DJ
 Callie L. Largent, DI
 Elizabeth R. Lavin, DC
 Kelly A. Mattes, DI

Kira M. McGovern, FE
Belynda F. Miller, PACOM
Elizabeth L. Neal, DC
Louane J. Powers, DX
Kimberly D. Robbins, HC
Monica C. Schroeder, DI
Rylan C. Vargas, SOCOM
Wayne Washington, FE
Lynn N. Willey, DI
Barbara J. Willis, DX

DIA Promotions to Pay Band 02

Dianna D. Cole, EUCOM
Brian L. Davis, JFCOM
Betty Diane Dillon, DX
Chi K. Etheridge, EUCOM
Susan G. Gatlin, DX
Nathan M. Pinkus, DH
Julio C. Rivera, CENTCOM
Rose M. Swinford, DX

Army Promotions

COL Shawn D. Fritz, DX
COL Michael J. Janser, DH

COL Michael E. Knutson, DX
COL Ivan B. Shidlovsky, J2
LTC Matthew D. Atkins, J2
LTC Hashem Bayatpoor, DX
LTC Charles O. Collins, DH
LTC Michelle L. Digruttolo, J2
LTC Scott T. Fleeher, DH
LTC Ricardo Gonzalez, DH
LTC Paul E. Lanzillotta, DI
LTC Jeffrey J. Monte, DX
LTC Edward P. O'Connor, DI
LTC Robert Schaefer, DX
LTC John W. Schurtz, DX
CPT Mark D. Little, HC
CW2 Paul D. Wilke, DX
MSG Kevin W. Allen, DH
MSG Armida Flores, DH
MSG Garrick L. Hipskind, DI
MSG Willie Lee Kelly Jr., DX
MSG Matthew A. Tuiasosopo, DX
SSG Joseph Betancourt, DS
SSG Curtis L. Curry, DX
SSG Timothy R. Branam, DI

Air Force Promotions

Col Jon Walker, DX
Lt Col Aaron Allgeyer, J2
Lt Col Edward Kaplan, J2
Lt Col Deborah MacKay, J2
Lt Col Scott Weston, DH
Maj Raymond Holstein, DI
Maj Lorenzo Slay, CE
Maj Michael Tyson, JMAS
SMSgt Judith Medeiros, DX
MSgt Michael Clutz, DI
MSgt Nancy Ganote, DJ
MSgt Brook Gebreyesus, DJ
TSgt Alon Molake, DH
SSgt Esther George, HC

Navy Promotions

CAPT Diego Corral, DH
CAPT Andrea Pollard, DI
CDR Paul C. Demarcus, DJ
CDR Richard J. LeGrande Jr., DH
LCDR Yerodin Mack, MC

Since our profile of Gwenie the Gosling in the July 6 InterComm, the Internal Communications office has been inundated with questions regarding Gwenie and her family's disappearance. For those who are concerned as to the whereabouts of DIA's resident fowl family, we have provide this response:

We in Internal Communications do not know where Gwenie and her family have gone.

But we have a theory.

After our interview and extensive photo shoot with Gwenie, the family received a lot of publicity. Gwenie's mom, Gertie, thought it was fantastic. The family was getting goose- and fowl-related issues out to the work force, and the goslings were being exposed to all different types of people, which she thought would help them grow up to be better geese. She had a nip and tuck to look better for her goslings' fans, and started styling her feathers differently.

However, Gwenie's father, Gustov, did not appreciate the publicity, saying that all the notoriety was damaging his goslings and their future. He threw a fit, honking and hissing at anyone that would come near. He even started seeing another goose on the side. He then decided to take his goslings to another pond far away from the DIAC for the winter and until their extensive home renovations were complete.

We're hoping that Gwenie, Gertie, Gustov and the rest of the gang come back in the spring. We miss them, too. Hopefully when springtime rolls around, they'll come back to the DIAC. Maybe we'll even have some grand-goslings running around the pond.

We hope this brought a little levity to your day.

— The Communiqué Staff



Photo by Margan C. Kerwin, CP

Gwenie's dad Gustov ushers his wife and goslings away from the flashing lights of the paparazzi. Gustov's dislike of the press is well-known to those in the Internal Communications office.

on the HORIZON

events for DECEMBER 2009 and JANUARY 2010

DECEMBER

Dec. 1 Chairman of the Joint Chiefs of Staff visits DIA, 8:30 a.m. to 10 a.m.

Dec. 1
Hanukkah begins at sunset

Dec. 7 DIA Holiday Party, 11 a.m. to 2 p.m., DIAC Cafeteria

Dec. 8 JFCC-ISR's Processing, Exploitation and Dissemination (PED) Working Group, Pentagon Room 1B688, 9 a.m. to 5 p.m.

Dec. 9 Hanukkah ends

Dec. 10 FEW Exec Board Meeting, noon to 1 p.m., Room TBD

Dec. 17 FEW Membership Meeting, 11:30 a.m. to 12:30 p.m., DIAC Room N-473

Dec. 14 Open season ends for Federal Employees Health Benefit, Dental and Vision Insurance programs and



Federal Flexible Spending Accounts

Dec. 15 HC and MC's CFC Piano/Vocal Concert, Tighe Auditorium

Dec. 15 CFC ends

Dec. 25 Christmas (observed)

Dec. 26 Kwanzaa

JANUARY

Jan. 1 New Year's Day (observed)

Jan. 5 HCL's Professional Development Day

Jan. 7
Clarendon Beverage Social, 11 a.m.

Jan. 12 Crystal Park 5 Beverage Social, 11 a.m.

Jan. 13 Operation Warfighter Career Fair and Luncheon, 9:30 a.m. to 2 p.m., DIAC



Jan. 14 Dorsey Park Beverage Social, 11 a.m.

Jan. 14 MSIC's MLK Birthday Celebration, Bob Johnson Auditorium, 10 a.m.

Jan. 14 FEW Exec Board Meeting, noon to 1 p.m., Room TBD

Jan. 18 Martin Luther King Jr. Day (observed)

Jan. 20 - 22 U.S. Forces Korea Conference, 8 a.m., DIAC

Jan. 21 Communications Board Meeting, 11:30 a.m. to 12:30 p.m., DIAC Room TBD

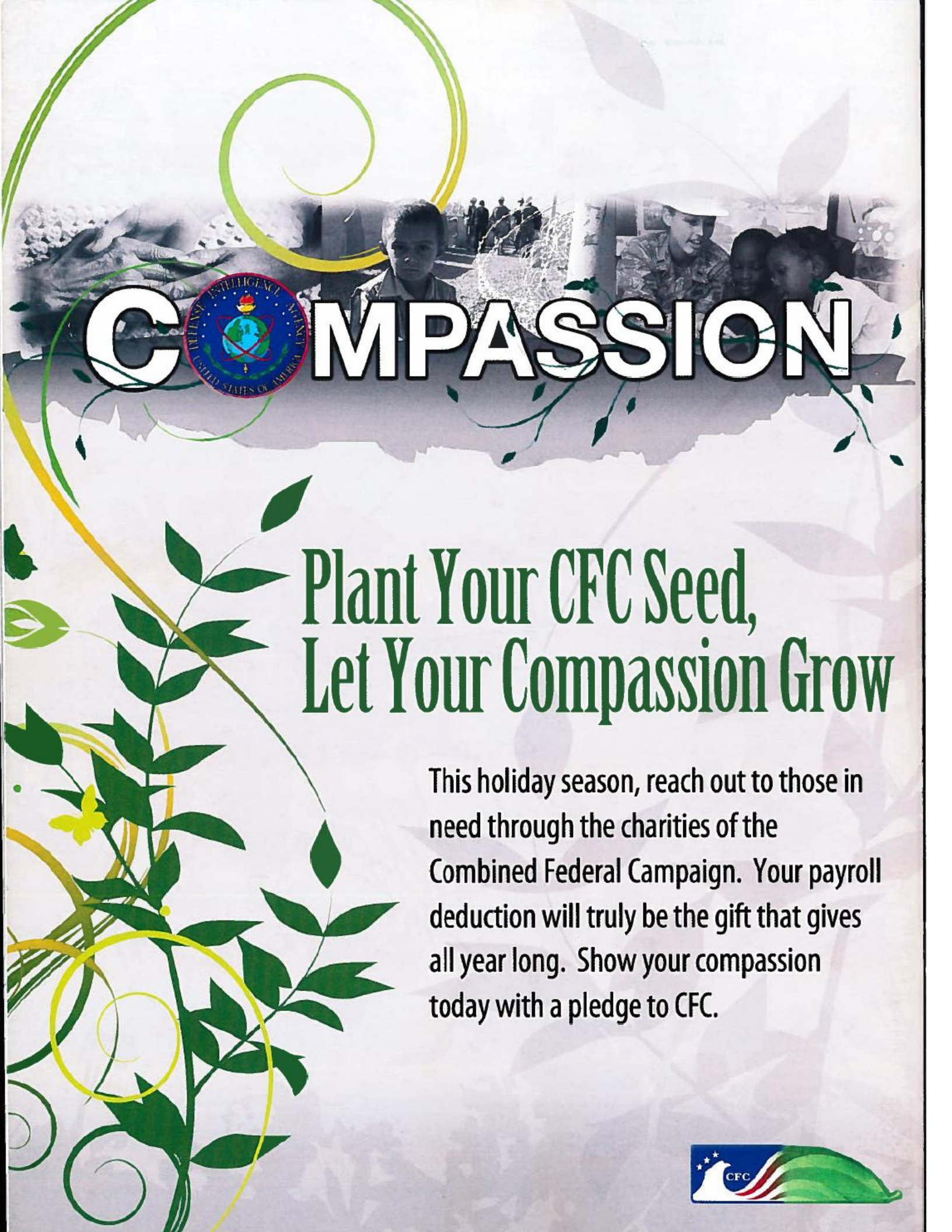
Jan. 21 Fair Oaks Beverage Social, 11 a.m.

Jan. 26 DX Beverage Social, 11 a.m.

Jan. 28 CWF Council Meeting, 9 a.m., DIAC



For further information or updates concerning these events, please refer to the Internal Communications Web site.



CMPASSION

Plant Your CFC Seed, Let Your Compassion Grow

This holiday season, reach out to those in need through the charities of the Combined Federal Campaign. Your payroll deduction will truly be the gift that gives all year long. Show your compassion today with a pledge to CFC.



